ESCUELA DE CIENCIAS JURÍDICAS

MÁSTER EXPERTO EN INFORMÁTICA Y ELECTRÓNICA FORENSE

JUR020

www.escuelacienciasjuridicas.com

Certificación universitaria internacional

Escuela asociada a:

DESTINATARIOS

El **Máster Informática Forense** está especialmente dirigido a todas aquellas personas que estén interesadas en ampliar sus conocimientos sobre la investigación de delitos informáticos. A lo largo del curso, el alumno estudiará los fundamentos de la informática y electrónica forense para peritar un dispositivo. Además, aprenderá técnicas de ciberseguridad y estudiará los aspectos relacionados con la cibercriminalidad y el hacking ético. Por otro lado, el estudiante se formará en el ámbito del análisis forense. Así, podrá aportar datos decisivos e importantes en el marco de la investigación de cualquier hecho delictivo, y siendo conocedor de estos conceptos, podrá escribir un informe pericial forense en informática. Finalmente, aprenderá la normativa sobre seguridad de la información vigente y los planes de acción para evitar y evaluar ataques informáticos.

MODALIDAD

• **A DISTANCIA:** una vez recibida tu matrícula, enviaremos a tu domicilio el pack formativo que consta de los manuales de estudio y del cuaderno de ejercicios.

DURACIÓN

La duración del curso es de 600h.

IMPORTE

Importe Original: ~~840€~~

Importe Actual: 420€

CERTIFICACIÓN OBTENIDA

Una vez finalizados los estudios y superadas las pruebas de evaluación, el alumno recibirá un diploma que certifica el "MÁSTER EXPERTO EN INFORMÁTICA Y ELECTRÓNICA FORENSE", de la ESCUELA DE CIENCIAS JURÍDICAS, avalada por nuestra condición de socios de la CECAP, máxima institución española en formación y de calidad.

Los diplomas, además, llevan el sello de Notario Europeo, que da fe de la validez de los contenidos y autenticidad del título a nivel nacional e internacional.

El alumno tiene la opción de solicitar junto a su diploma un Carné Acreditativo de la formación firmado y sellado por la escuela, válido para demostrar los contenidos adquiridos.

Además, el alumno podrá solicitar una Certificación Universitaria Internacional de la Universidad Católica de Cuyo-DQ con un reconocimiento de 24 ECTS.

CONTENIDO FORMATIVO

MÓDULO 1. INFORMÁTICA Y ELECTRÓNICA FORENSE

UNIDAD DIDÁCTICA 1. INFORMÁTICA, CONECTIVIDAD E INTERNET

1. La informática
   - Conceptos básicos
2. Componentes de un sistema informático
3. Estructura básica de un sistema informático
4. Unidad central de proceso en un sistema informático
   - Estructura
5. Periféricos más usuales: conexión
6. Sistema operativo
7. Internet
8. Conectividad a Internet
   - Tipos de redes
   - 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
   - Evidencias volátiles y no volátiles
   - Etiquetado de evidencias
7. Cadena de custodia

UNIDAD DIDÁCTICA 3. CIBERSEGURIDAD

1. El ciberespacio y su seguridad
2. Riesgos y amenazas de la ciberseguridad
   - Amenazas internas y externas
   - 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
   - Principales características del delito informático
2. Tipos de delito informático
3. Cibercriminalidad
   - 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?
   - Ética hacker
   - Valores de la ética hacker
   - Fases del Hacking Ético
   - Tipo de Hacking Ético
2. Aspectos legales del hacking ético
3. Perfiles del hacker
   - Hacker de sombrero negro
   - Hacker de sombrero blanco
   - Hacker de sombrero gris
   - Otros perfiles
4. Hacktivismo

UNIDAD DIDÁCTICA 6. ANÁLISIS FORENSE

1. El análisis forense
2. Etapas de un análisis forense
   - Estudio preliminar
   - Adquisición de datos
   - Análisis e investigación
   - 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
   - Dinámica del borrado de archivos
   - Características exigibles para recuperación de archivos y datos borrados
   - Principales herramientas para recuperación de datos
   - La acción de recuperación
4. Análisis de archivos
   - Firmas características
   - Documentos
   - Archivos gráficos y multimedia
   - 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
   - Principio Básico de Confidencialidad
   - Principio Básico de Integridad
   - 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
   - Planes de acción para la utilización más segura de Internet
   - Estrategias para una sociedad de la información más segura
   - Ataques contra los sistemas de información
   - La lucha contra los delitos informáticos
   - La Agencia Europea de Seguridad de las Redes y de la información (ENISA)
3. Normativa relacionada con la ciberseguridad
4. Legislación sobre delitos informáticos

MÓDULO 2. ADMINISTRACIÓN ELECTRÓNICA