Curso online: Especialista en Informática y Electrónica Forense

Working
Formación Integral S.L.

www.workingformacion.com

OBJETIVOS

La informática forense aparece para enfrentar los desafíos y técnicas de los intrusos informáticos, así como defensora de la verdad alrededor de la evidencia digital. A través de este pack de materiales didácticos el alumnado podrá adquirir las competencias profesionales necesarias para profundizar en lo que la informática forense se refiere.

CONTENIDOS

UNIDAD DIDÁCTICA 1. INFORMÁTICA, CONECTIVIDAD E INTERNET

1. La informática
2. Conceptos básicos
3. Componentes de un sistema informático
4. Estructura básica de un sistema informático
5. Unidad central de proceso en un sistema informático
6. Estructura
7. Periféricos más usuales: conexión
8. Sistema operativo
9. Internet
10. Conectividad a Internet
11. Tipos de redes
12. 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
7. Evidencias volátiles y no volátiles
8. Etiquetado de evidencias
9. Cadena de custodia

UNIDAD DIDÁCTICA 3. CIBERSEGURIDAD

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

UNIDAD DIDÁCTICA 4. CIBERCRIMINALIDAD

1. Delito informático
2. Principales características del delito informático
3. Tipos de delito informático
4. Cibercriminalidad
5. 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?
2. Ética hacker
3. Valores de la ética hacker
4. Fases del Hacking Ético
5. Tipo de Hacking Ético
6. Aspectos legales del hacking ético
7. Perfiles del hacker
8. Hacker de sombrero negro
9. Hacker de sombrero blanco
10. Hacker de sombrero gris
11. Otros perfiles
12. Hacktivismo

UNIDAD DIDÁCTICA 6. ANÁLISIS FORENSE

1. El análisis forense
2. Etapas de un análisis forense
3. Estudio preliminar

4. Adquisición de datos
5. Análisis e investigación
6. Presentación y realización del informe pericial
7. Tipos de análisis forense
8. Requisitos para el análisis forense
9. 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
4. Dinámica del borrado de archivos
5. Características exigibles para recuperación de archivos y datos borrados
6. Principales herramientas para recuperación de datos
7. La acción de recuperación
8. Análisis de archivos
9. Firmas características
10. Documentos
11. Archivos gráficos y multimedia
12. 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
5. - Principio Básico de Confidencialidad
6. - Principio Básico de Integridad
7. - Disponibilidad
8. Descripción de los riesgos de la seguridad
9. Selección de controles

10. Factores de éxito en la seguridad de la información
11. Introducción a los sistemas de gestión de seguridad de la información
12. 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
3. Planes de acción para la utilización más segura de Internet
4. Estrategias para una sociedad de la información más segura
5. La lucha contra los delitos informáticos
6. La Agencia Europea de Seguridad de las Redes y de la información (ENISA)
7. Normativa relacionada con la ciberseguridad
8. Legislación sobre delitos informáticos

MODALIDAD

METODOLOGÍA

Online. Se entrega el material a través de nuestra plataforma virtual homologada. Contará con acceso a la misma las 24 horas al día los 365 días del año.

http://cursosonline.workingformacion.com

DURACIÓN

200 horas

IMPARTIDO POR

Tutor experto en la materia. Contará con apoyo a través de nuestra plataforma en todo momento.

Al finalizar el curso se hará entrega de un
DIPLOMA HOMOLOGADO

Working

Formación Integral S.L.

Paseo Rosales 32, local 9 50008 Zaragoza
976 242 109 - info@workingformacion.com

www.workingformacion.com