CIBERSEGURIDAD, CRIPTOGRAFÍA, Y DELITOS TELEMÁTICOS

CIBERSEGURIDAD, CRIPTOGRAFÍA, Y DELITOS TELEMÁTICOS

Duración: 60 horas

Precio: consultar euros.

Modalidad: e-learning

Objetivos:

Descripción: Aprender los conceptos fundamentales en materia de ciberseguridad, las amenazas y vulnerabilidades más importantes y la estrategia de respuesta a los ciberataques. 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.

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.

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. CONCEPTOS BASICOS SOBRE LA SEGURIDAD DE COMUNICACIONES Y CRIPTOGRAFIA

1. CONCEPTOS BÁSICOS DE CRIPTOGRAFÍA
2. OBJETIVOS DE SEGURIDAD CRIPTOGRÁFICA
3. CONCEPTOS BÁSICOS DE CRIPTOGRAFÍA
4. ¿QUÉ ES ENCRIPTACIÓN?
5. ASEGURANDO DATOS CON ALGORITMOS CRIPTOGRÁFICOS
6. CIFRAR DATOS ALMACENADOS EN DISCO
7. INTRODUCCIÓN A LA ESTEGANOGRAFÍA
8. MODELO DEL ESTEGANOSISTEMA
9. USO DE LA ESTEGANOGRAFÍA
10. CLASIFICACIÓN DE LA ESTEGANOGRAFÍA
11. EL ARCHIVO DIGITAL
12. SISTEMA DE FICHEROS ESTEGANOGRÁFICO

TEMA 2. MALWARE, HACKING Y DDOS

1. HACKING
2. MALWARE
3. HISTORIA DE LOS VIRUS Y GUSANOS
4. SPAM
5. RANSOMWARE Y EL SECUESTRO DE INFORMACIÓN
6. VIRUS
7. HOAX
8. BOMBAS LÓGICAS
9. CABALLOS DE TROYA
10. GUSANOS
11. CONTRAMEDIDAS
12. NEGACIÓN DE SERVICIO
13. CÓMO FUNCIONAN LOS ATAQUES DDOS
14. COMO TRABAJA BOTS/BOTNETS
15. ATAQUES SMURF E INUNDACIÓN DE SYN

16. TEARDROP
17. LAND
18. ENVENENAMIENTO DNS
19. PING DE LA MUERTE
20. CONTRAMEDIDAS PARA DOS/DDOS
21. PELIGROS PLANTEADOS POR EL SECUESTRO DE SESIÓN

TEMA 3. HARDENING

1. CONCEPTOS Y PRINCIPIOS DE LA ADMINISTRACIÓN DE LA SEGURIDAD
2. MECANISMOS DE PROTECCIÓN
3. CONTROL/GESTIÓN DE CAMBIOS
4. CONCEPTOS DE SEGURIDAD OPERACIONAL
5. CONTROL DE PERSONAL

TEMA 4. AUDITORIA Y DETECCION DE INTRUSOS

1. AUDITORÍA
2. MONITORIZACIÓN
3. TÉCNICAS DE PRUEBAS DE PENETRACIÓN
4. ACTIVIDADES INAPROPIADAS
5. AMENAZAS Y CONTRAMEDIDAS INDISTINTAS
6. SISTEMAS DE DETECCIÓN DE INTRUSOS

TEMA 5. DELITOS TIPIFICADOS Y FICHAS TECNICAS DE LOS DELITOS TIPIFICADOS

1. PRINCIPALES CATEGORÍAS DE CRÍMENES DE ORDENADOR
2. ACTIVIDAD CRIMINAL A TRAVÉS DE WEB
3. ROBO DE INFORMACIÓN, MANIPULACIÓN DE DATOS USURPACIÓN DE WEB
4. TERRORISMO
5. CRÍMENES NEOTRADICIONALES: VINO VIEJO EN NUEVAS BOTELLAS
6. LAVADO DE DINERO