

CURSO FORMATIVO CIBERSEGURIDAD

Coordinador Académico
Alfonso Muñoz

Conecta Empleo

Contenido desarrollado por **Telefónica Educación Digital**



Índice

1.	PRESENTACIÓN Y OBJETIVOS	03
2.	¿QUÉ VAS A APRENDER?	03
3.	¿CÓMO SE ESTUDIA?	03
4.	FORMACIÓN CIBERSEGURIDAD	04
4.1	Ciberseguridad	05
4.2	Formación de habilidades para la empleabilidad	07

1. PRESENTACIÓN Y OBJETIVOS

2. ¿QUÉ VAS A APRENDER?

3. ¿CÓMO SE ESTUDIA?

-Con esta formación vas a adquirir las competencias de una de las especializaciones técnicas más demandadas y con más futuro en el mercado laboral actual. Con este curso serás capaz de introducirte con unas bases de conocimiento sólidas en el mundo de la Ciberseguridad. Como punto de partida tenemos Redes y Sistemas, y como cierre ataques a infraestructuras y Hacking Ético.

- Conceptos básicos de Ciberseguridad
- Programar de forma segura
- Técnicas de protección para infraestructuras
- Contramedidas
- Ataques a infraestructuras
- Hacking ético

Todos los módulos formativos son Presenciales y además seguirás formándote fuera del aula. Las impartición de las clases presenciales será de Lunes a Viernes, 5 horas diarias.



Contenidos Virtuales

Desde el inicio podrás acceder a toda la documentación de las diferentes materias y ejercicios prácticos, recursos extra de apoyo académico (vídeos, bibliografía, links, etc.).



Sesiones de Valor Añadido

Masterclasses, invitaciones a Foros de Empleo, Sesiones de trabajo con profesionales de las Empresas Colaboradoras.



Networking

Tendrás posibilidad de ampliar tu red de contactos con otros participantes, expertos, gurús, profesionales digitales.



Acompañamiento Individual

Dispondrás de tutorías, sesiones de orientación laboral y mentoring tanto durante la fase de Formación como en la fase de incorporación laboral.



Casos prácticos reales

Aprenderás trabajando sobre proyectos reales, los casos que trabajarás durante el programa pertenecen a situaciones que se dan diariamente en empresas punteras del sector. Formación orientada a la realidad laboral.



Portfolio de actividades

Al final del programa contarás con un portfolio de actividades en el que se recogerán todos los casos prácticos realizados durante tu formación. Qué mejor curriculum que mostrar lo que sabes hacer.

4. FORMACIÓN: CIBERSEGURIDAD



FORMACIÓN EN CIBERSEGURIDAD

Redes y Aplicaciones técnicas

Análisis Forense de
Sistemas Informáticos

Hacking con Python

Hacking Ético

Gobierno y Riesgos

Metasploit

Criptografía / Esteganografía

Vulneración Mecanismos
Identificación y autenticación

Desarrollo de un proyecto
transversal al curso

Formación en habilidades
para la empleabilidad

4. FORMACIÓN: CIBERSEGURIDAD



FORMACIÓN EN CIBERSEGURIDAD

Duración 250 horas

REDES Y APLICACIONES TÉCNICAS

Comprender los conocimientos básicos y de las herramientas necesarias para realizar diversas tareas de seguridad relacionadas.
CONCEPTOS: Arquitectura OSI y TCP/IP, Dispositivos de red, Arquitectura de red, MAC/CAM y MITM Ataques DHCP, SLAAC y Spoofing, seguridad Wireless

HACKING CON PYTHON

Conocer el lenguaje de programación Python, así como aportar al alumno de los conocimientos básicos y de las herramientas necesarias para realizar diversas tareas de Seguridad
CONCEPTOS: geolocalización IP, recolección de información usando shodan, pastebin, análisis/detección de vulnerabilidades, ataques básicos a nivel de red

GOBIERNO Y RIESGOS

Comprender el amplio mundo de la ciberseguridad, y todas las posibilidades que abarca.
CONCEPTOS: Roles y responsabilidades, Malware y tendencias, Gestión y gobierno del riesgo, Gestión de la seguridad, Respuesta ante incidente,

CRİPTOGRAFÍA / ESTEGANOGRAFÍA

Comprender entender nuevos mecanismos de protección de comunicaciones digitales.
CONCEPTOS: Seguridad y criptografía, Aritmética modular, historia de la criptografía y la cifra clásica, algoritmos de cifra simétrica en flujo y en bloque, funciones hash, algoritmos de cifra asimétrica, Esteganografía.

ANÁLISIS FORENSE DE SISTEMAS INFORMÁTICOS

Conocer el análisis forense y los procedimientos para adquisición y conservación de evidencias digitales
CONCEPTOS: Clonación, integridad, logs y tráfico de red, prevención de intrusiones, gestión y análisis de logs de Windows

4. FORMACIÓN: CIBERSEGURIDAD



FORMACIÓN EN CIBERSEGURIDAD

Duración 250 horas

HACKING ÉTICO

Conocer y comprender las técnicas principales para realizar un hacking ético a un sistema

CONCEPTOS: Hacking ético, footprinting, fingerprinting, sniffing, enumeración, análisis de vulnerabilidades, explotación de vulnerabilidades, estándares y modelos, vulnerabilidades web, ingeniería social, DoS, malware

METASPLOIT

Conocer y realizar un proceso de pentesting, mediante el uso de Metasploit

CONCEPTOS: Hacking Ético, técnicas de explotación y vulneración, uso y manipulación con Metasploit Framework.

VULNERACIÓN DE MECANISMOS DE IDENTIFICACIÓN Y AUTENTICACIÓN

Conocer las principales técnicas de identificación y autenticación como son las técnicas de control de acceso.

CONCEPTOS: Técnicas de identificación y autenticación, ciclo de vida de la identidad digital, control de acceso.

DESARROLLO DE UN PROYECTO

Desarrollar un trabajo final relacionado con la ciberseguridad de manera transversal durante el curso.

CONCEPTOS: Aplicación de los conceptos y tecnologías estudiadas en el curso.

4. FORMACIÓN: CIBERSEGURIDAD



4.3 FORMACIÓN DE HABILIDADES PARA LA EMPLEABILIDAD Duración 20 horas

• Para potenciar todos los conocimientos técnicos aprendidos tendrás un Módulo de Formación en Habilidades a lo largo de todo el itinerario formativo:

- Incrementar las competencias profesionales.
- Desarrollo de Inteligencia Emocional.
- Presentaciones Eficaces.
- Trabajo en Equipo
- Marca Personal y búsqueda de empleo 2.0
- Realizar entrevistas de trabajo de manera efectiva.

Conecta Empleo

