# 4. Fuentes de información (cursos no gratuitos)

## 4.1 Cursos no gratuitos sobre el tipo de tecnología en general

### 4.1.1 Curso no gratuito 1 sobre el tipo de tecnología en general

La Universidad de Alcalá ofrece un curso de verano sobre seguridad informática.

<https://drive.google.com/file/d/1ZigZtNe9n0O0CVaO877oxbGJQhh3Idrx/view>

Objetivos:

Formar a los alumnos en conceptos y herramientas avanzadas en ciberseguridad, desarrollo y aprendizaje de herramientas para hacking, redes sociales y redes TOR (Deep web)

### 4.1.2 Curso no gratuito 2 sobre el tipo de tecnología en general

<https://thesecuritysentinel.es/curso/certificado-profesional-de-hacking-etico/>

* Este curso te proporciona los conocimientos necesarios a nivel conceptual y práctico para que puedas implementar en empresas y negocios, un sistema Integral de Seguridad Informática integral y perimetral, apoyado por el uso de Software Libre.
* Desarrollarás y adquirirás habilidades prácticas para la realización de auditorías de sistemas intrusivos, usando las técnicas de la Auditoria de T.I del tipo “Hacking Ético y/o Test de Penetración”.
* Conocerás los diferentes tipos de atacantes, así como a usar las diferentes técnicas y herramientas de intrusión utilizadas por los delincuentes informáticos para lograr violentar la seguridad de un sistema de información.
* Con este curso, podrás realizar sin problemas auditorías de Pentesting con su correspondiente informe profesional, además de conocer los métodos utilizados por los delincuentes cibernéticos para poder contrarrestar sus ataques.
* Este curso se ha definido con un 75% de práctica y un 25 % de teoría, lo que te facilitará mucho el aprendizaje y el aprovechamiento máximo de conocimientos.
* Orientar las auditorias intrusivas haciendo uso de las normas y buenas prácticas en seguridad de la información a nivel internacional.
* Aprender las técnicas de ataque y protección de las redes inalámbricas y las aplicaciones web dinámicas.
* Formar auditores técnicos e integrales en el tema de seguridad de la información.

### 4.1.3 Curso no gratuito 3 sobre el tipo de tecnología en general

<https://www.udemy.com/kali-linux-pruebas-de-penetracion-y-hacking-etico-basico/?siteID=ycsZhk7mqJY-dLiMITU0NxTuFVAgSj.pcw&LSNPUBID=ycsZhk7mqJY>

En este curso el alumno aprenderá algunas de las técnicas básicas de Hacking Ético y Pruebas de Penetración en un entorno de pruebas de práctica 100% seguro.

El alumno comprenderá el potencial de Kali Linux y las herramientas que posee para realizar Pruebas de Penetración y Hacking Ético explotando software vulnerable y obteniendo una consola remota.

### 4.1.4 Curso no gratuito 4 sobre el tipo de tecnología en general

<https://www.imf-formacion.com/masters-profesionales/master-seguridad-informatica-presencial>

### **OBJETIVOS DEL MÁSTER EN CIBERSEGURIDAD PRESENCIAL**

Dotar al alumno de un conocimiento amplio y riguroso en disciplinas tales como **ciberinteligencia, análisis de malware, auditorías técnicas de redes y sistemas (hacking ético), análisis forense y gestión de incidentes de seguridad, desarrollo seguro de aplicaciones web y la monitorización y correlación de eventos de seguridad** (por medio de tecnologías SIEM).

Los objetivos específicos que logrará el alumno son los siguientes:

* Obtener una visión global del ámbito de la ciberseguridad, conociendo los ataques más relevantes y cómo mitigarlos.
* Desarrollar competencias técnicas y aprender a usar herramientas que exploten al máximo sus conocimientos y habilidades para la realización de pruebas de intrusión en redes y sistemas.
* Adquirir la capacitación necesaria para obtener, mantener y procesar evidencias digitales usando herramientas y procedimientos específicos.
* Conocer el mundo de la ingeniería inversa y analizar código malicioso, asumiendo los procesos para comprender el funcionamiento de los ficheros que trabajan a bajo nivel en sistemas y redes.
* Asimilar los conocimientos precisos para gestionar y establecer políticas claras de seguridad para el componente móvil de los sistemas.
* Conocer de forma práctica los principios de la monitorización y correlación de eventos de seguridad, a través de informes reales.
* Formarse como desarrollador en programación segura y mejorar sus habilidades como auditor de seguridad en el análisis y evaluación del código fuente de las aplicaciones.

### 4.1.5 Curso no gratuito 5 sobre el tipo de tecnología en general

<https://www.akademus.es/cursos/hacking-etico-cero-cien/>

- Este curso te proporciona los conocimientos necesarios a nivel conceptual y práctico para que puedas implementar en empresas y negocios, un sistema integral de seguridad informática integral y perimetral, apoyado por el uso de Software libre.

- Desarrollarás y adquirirás habilidades prácticas para la realización de auditorías de sistemas intrusivos, usando las técnicas de la Auditoría de T.I del tipo "Hacking Ético y/o Test de Penetración".

- Conocerás los diferentes tipos de atacantes, así como a usar las diferentes técnicas y herramientas de intrusión utilizadas por los delincuentes informáticos para lograr violentar la seguridad de un sistema de información.

- Con este curso, podrás realizar sin problemas auditorías de Pentesting con su correspondiente informe profesional, además de conocer los métodos utilizados por los delincuentes cibernéticos para poder contrarrestar sus ataques.

### 4.1.6 Curso no gratuito 6 sobre el tipo de tecnología en general

<https://cursos.securizame.com/courses/hacking-etico/>

En el curso se tratarán los principales temas relacionados con el hacking ético desde diferentes puntos de vista, permitiendo al alumno comprender y aprender a realizar test de intrusión para poder emitir conclusiones y minimizar los riesgos asociados en la exposición de un sistema informático a Internet, realización de auditoría interna, redes inalámbricas, etc,…

El curso tendrá una duración de **56 horas** y está orientado a auditores, administradores de sistemas y especialistas en el sector de seguridad, con un conocimiento medio. Dado que se empezará con una introducción al hacking ético, también es accesible a aquellos profesionales que deseen iniciarse en el sector adquiriendo, al final del curso un muy buen nivel de conocimientos.