Contenido

[1. Autores del trabajo, planificación y entrega 3](#_Toc444537686)

[1.1 Autores 3](#_Toc444537687)

[1.2 Planificación 3](#_Toc444537688)

[1.3 Entrega 3](#_Toc444537689)

[2. Descripción del tipo de tecnología 3](#_Toc444537690)

[3. Fuentes de información (documentos) 3](#_Toc444537691)

[3.1 Fuentes sobre el tipo de tecnología en general 4](#_Toc444537692)

[3.1.1 Fuente de información 1 sobre el tipo de tecnología en general 4](#_Toc444537693)

[3.1.2 Fuente de información 2 sobre el tipo de tecnología en general 4](#_Toc444537694)

[3.1.n Fuente de información n sobre el tipo de tecnología en general 4](#_Toc444537695)

[3.2 Fuentes sobre la tecnología específica A 4](#_Toc444537696)

[3.2.1 Fuente de información 1 sobre la tecnología específica A 4](#_Toc444537697)

[3.2.2 Fuente de información 2 sobre la tecnología específica A 4](#_Toc444537698)

[3.2.n Fuente de información n sobre la tecnología específica A 4](#_Toc444537699)

[3.3 Fuentes sobre la tecnología específica B 4](#_Toc444537700)

[3.3.1 Fuente de información 1 sobre la tecnología específica B 4](#_Toc444537701)

[3.3.2 Fuente de información 2 sobre la tecnología específica B 4](#_Toc444537702)

[3.3.n Fuente de información n sobre la tecnología específica B 4](#_Toc444537703)

[4. Fuentes de información (cursos no gratuitos) 4](#_Toc444537704)

[4.1 Cursos no gratuitos sobre el tipo de tecnología en general 4](#_Toc444537705)

[4.1.1 Curso no gratuito 1 sobre el tipo de tecnología en general 4](#_Toc444537706)

[4.1.2 Curso no gratuito 2 sobre el tipo de tecnología en general 4](#_Toc444537707)

[4.1.n Curso no gratuito n sobre el tipo de tecnología en general 4](#_Toc444537708)

[4.2 Cursos no gratuitos sobre la tecnología específica A 4](#_Toc444537709)

[4.2.1 Curso no gratuito 1 sobre la tecnología específica A 4](#_Toc444537710)

[4.2.2 Curso no gratuito 2 sobre la tecnología específica A 4](#_Toc444537711)

[4.2.n Curso no gratuito n sobre la tecnología específica A 4](#_Toc444537712)

[4.3 Cursos no gratuitos sobre la tecnología específica B 5](#_Toc444537713)

[4.3.1 Curso no gratuito 1 sobre la tecnología específica B 5](#_Toc444537714)

[4.3.2 Curso no gratuito 2 sobre la tecnología específica B 5](#_Toc444537715)

[4.3.n Curso no gratuito n sobre la tecnología específica B 5](#_Toc444537716)

[5. Fuentes de información (cursos gratuitos) 5](#_Toc444537717)

[5.1 Cursos gratuitos sobre el tipo de tecnología en general 5](#_Toc444537718)

[5.1.1 Curso gratuito 1 sobre el tipo de tecnología en general 5](#_Toc444537719)

[5.1.2 Curso gratuito 2 sobre el tipo de tecnología en general 5](#_Toc444537720)

[5.1.n Curso gratuito n sobre el tipo de tecnología en general 5](#_Toc444537721)

[5.2 Cursos gratuitos sobre la tecnología específica A 5](#_Toc444537722)

[5.2.1 Curso gratuito 1 sobre la tecnología específica A 5](#_Toc444537723)

[5.2.2 Curso gratuito 2 sobre la tecnología específica A 5](#_Toc444537724)

[5.2.n Curso gratuito n sobre la tecnología especifica A 5](#_Toc444537725)

[5.3 Cursos gratuitos sobre la tecnología específica B 5](#_Toc444537726)

[5.3.1 Curso gratuito 1 sobre la tecnología específica B 5](#_Toc444537727)

[5.3.2 Curso gratuito 2 sobre la tecnología específica B 5](#_Toc444537728)

[5.3.n Curso gratuito n sobre la tecnología especifica B 5](#_Toc444537729)

[6. Ayudas para estudiar las tecnologías 5](#_Toc444537730)

[7. Recursos para implementar las tecnologías 6](#_Toc444537731)

[7.1 Recursos para implementar la tecnología A 6](#_Toc444537732)

[7.1.1 Recursos no gratuitos para implementar la tecnología A 6](#_Toc444537733)

[7.1.1 Recursos no gratuitos para implementar la tecnología A 6](#_Toc444537734)

[7.2 Recursos para implementar la tecnología B 6](#_Toc444537735)

[7.2.1 Recursos no gratuitos para implementar la tecnología B 6](#_Toc444537736)

[7.2.1 Recursos no gratuitos para implementar la tecnología B 6](#_Toc444537737)

[8. Conclusiones 6](#_Toc444537738)

# 1. Autores del trabajo, planificación y entrega

## 1.1 Autores

En este apartado se debe indicar el número de grupo y los nombres de los autores, poniendo en primer lugar al coordinador del grupo.

## 1.2 Planificación

En este apartado se debe incluir un enlace (URL) compartido a la planificación del trabajo utilizando una herramienta online de diagramación Gantt (por ejemplo, GanttPro, versión gratuita).

En este enlace hay un ejemplo de una posible planificación del trabajo, que se puede usar como referencia, pero indicando los nombres reales de las tecnologías y de los participantes.

[Ejemplo planificación](https://app.ganttpro.com/shared/token/b0b82a0da290d4dcc93d8813795ad00093b8c583b346f796b38148ef71895eb1#!/app/home).

Hay que tener en cuenta que, como puede verse en el ejemplo, cada participante del grupo debe tener asignadas tareas que sumen al menos 15 horas. El peso de este trabajo en la calificación total de la asignatura es de un 10%, por tanto requiere de una dedicación de 15 horas del total de 150 horas de la asignatura.

## 1.3 Entrega

En este apartado debe incluirse un enlace (URL) a un repositorio en GitHub o en BitBucket creado para el trabajo.

En dicho repositorio debe encontrarse, al menos los siguientes archivos en la rama máster:

* Trabajo terminado: del trabajo terminado con el nombre TG1\_final.ocx
* Presentación del trabajo: TG1\_final.pptx

Dichos archivos serán los que se tendrán en cuenta para la calificación del trabajo.

# 2. Descripción del tipo de tecnología

En este apartado se debe indicar el tipo de tecnología en general y las tecnologías específicas sobre las que trata el trabajo.

El objetivo del trabajo es ponerse en la situación de una persona ya titulada en el Grado en Sistemas de Información, y que desea actualiza sus conocimientos sobre dichas tecnologías.

En este documento se debe recoger toda la información que se ha recopilado para poder aprender la teoría y práctica de dichas tecnologías, así como las ayudas que existen para poder financiar su estudio o su implementación en empresas u otras organizaciones.

# 3. Fuentes de información (documentos)

En los sub-apartados de este apartado se deben indicar documentos de interés para aprender sobre el tipo de tecnología en general, y sobre cada una de las tecnologías elegidas.

Sobre cada documento se debe

## 3.1 Fuentes sobre el tipo de tecnología en general

### 3.1.1 Fuente de información 1 sobre el tipo de tecnología en general

En la página web <https://docs.kali.org/> encontramos la documentación oficial sobre Kali Linux. Se trata de una distribución GNU/Linux con más de 300 herramientas y aplicaciones relacionadas con la seguridad informática, destacando algunas tan conocidas como *Nmap*, que permite escanear los puertos de un sistema, el crackeador de contraseñas *John the Ripper* o la suite *Aircrack-ng* para comprobar la seguridad de las redes inalámbricas.

### 3.1.2 Fuente de información 2 sobre el tipo de tecnología en general

En la página web <https://www.dragonjar.org/> ofrecen gran cantidad de contenido sobre seguridad informática, tutoriales, formación, foros, etc. La Comunidad DragonJAR, una de las comunidades de habla hispana referentes en el área de seguridad informática, y que en más de 15 años se ha caracterizado por ser el semillero virtual para quienes hoy son grandes profesionales en el ámbito de la seguridad informática, tanto en Colombia cómo en Latinoamérica.

Escribiendo la palabra *passwords* en su buscador nos aparecen varios enlaces a posts relacionados con el cracking de contraseñas.

### 3.1.3 Fuente de información 3 sobre el tipo de tecnología en general

<http://www.securitybydefault.com/> se trata de un blog donde se habla íntegramente sobre seguridad informática, un espacio donde profesionales comparten experiencias y hablan de los aspectos técnicos relacionados con la seguridad informática.

### 3.1.4 Fuente de información 4 sobre el tipo de tecnología en general

En el siguiente enlace <https://www.ma.rhul.ac.uk/static/techrep/2013/MA-2013-07.pdf> encontramos una tesis del autor Chrysanthou Yiannis de la Royal Holloway University of London, donde se explican las formas más populares de crackeo de contraseñas, además de desarrollar una técnica propia del autor.

### 3.1.5 Fuente de información 5 sobre el tipo de tecnología en general

<https://www.youtube.com/watch?v=xhz_w_iZtVE>

En este enlace accedemos a una ponencia de Passwordscon in Las Vegas, donde vemos cómo las matemáticas y la estadística pueden ayudar al crackeo de contraseñas. Se explica como ejemplo la técnica de Markov.

## 3.2 Fuentes sobre la tecnología específica A

### 3.2.1 Fuente de información 1 sobre la tecnología específica A

### 3.2.2 Fuente de información 2 sobre la tecnología específica A

### 3.2.n Fuente de información n sobre la tecnología específica A

## 3.3 Fuentes sobre la tecnología específica B

### 3.3.1 Fuente de información 1 sobre la tecnología específica B

### 3.3.2 Fuente de información 2 sobre la tecnología específica B

### 3.3.n Fuente de información n sobre la tecnología específica B

# 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.

## 4.2 Cursos no gratuitos sobre la tecnología específica A

### 4.2.1 Curso no gratuito 1 sobre la tecnología específica A

### 4.2.2 Curso no gratuito 2 sobre la tecnología específica A

### 4.2.n Curso no gratuito n sobre la tecnología específica A

## 4.3 Cursos no gratuitos sobre la tecnología específica B

### 4.3.1 Curso no gratuito 1 sobre la tecnología específica B

### 4.3.2 Curso no gratuito 2 sobre la tecnología específica B

### 4.3.n Curso no gratuito n sobre la tecnología específica B

# 5. Fuentes de información (cursos gratuitos)

## 5.1 Cursos gratuitos sobre el tipo de tecnología en general

### 5.1.1 Curso gratuito 1 sobre el tipo de tecnología en general

<https://miriadax.net/web/seguridad-informatica-practica/inicio?timestamp>=

El curso está diseñado para introducir al alumno en el autoaprendizaje práctico de la seguridad, de forma que, progresivamente, adquiera la experiencia necesaria para poder plantear y llevar a cabo sus propios ejercicios y pruebas. El curso incluye demostraciones y ejercicios que los estudiantes pueden reproducir y realizar en su propio ordenador, usando para ello el laboratorio NETinVM (http://netinvm.org).

### 5.1.2 Curso gratuito 2 sobre el tipo de tecnología en general

<http://www.esetec.es/cursos/seguridad-informatica>

Este **curso de Seguridad informática**te permitirá garantizar la seguridad de los accesos y usos de la información registrada en equipos informáticos, así como del propio sistema, protegiéndose de los posibles ataques, identificando vulnerabilidades y aplicando sistemas de cifrado a las comunicaciones que se realicen hacia el exterior y en el interior de la organización.

### 5.1.3 Curso gratuito 3 sobre el tipo de tecnología en general

<http://190.90.112.209/Primer_curso_de_cracking_de_Ricardo_Narvaja_completo.pdf>

Se explica en un curso sencillo las bases para crackear programas o mejor expresado las bases de la INGENIERIA REVERSIBLE que es el arte de revertir las protecciones que poseen ciertos programas para hacerlos accesibles a todos y no haya que pagar por usarlos.

### 5.1.4 Curso gratuito 4 sobre el tipo de tecnología en general

<https://edutin.com/curso-de-hacking-3106>

Este curso gratis de programación Hacking te dará oportunidades de conocer como son los defectos de las páginas web, cuáles son sus mecanismos de seguridad, y también a protegerte de los conocedores del campo del hacking.

## 5.2 Cursos gratuitos sobre la tecnología específica A

### 5.2.1 Curso gratuito 1 sobre la tecnología específica A

### 5.2.2 Curso gratuito 2 sobre la tecnología específica A

### 5.2.n Curso gratuito n sobre la tecnología especifica A

## 5.3 Cursos gratuitos sobre la tecnología específica B

### 5.3.1 Curso gratuito 1 sobre la tecnología específica B

### 5.3.2 Curso gratuito 2 sobre la tecnología específica B

### 5.3.n Curso gratuito n sobre la tecnología especifica B

# 6. Ayudas económicas para estudiar las tecnologías

# 7. Recursos para implementar las tecnologías

## 7.1 Recursos para implementar la tecnología A

### 7.1.1 Recursos gratuitos para implementar la tecnología A

### 7.1.2 Recursos no gratuitos para implementar la tecnología A

## 7.2 Recursos para implementar la tecnología B

### 7.2.1 Recursos gratuitos para implementar la tecnología B

### 7.2.2 Recursos no gratuitos para implementar la tecnología B

# 8. Conclusiones