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

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

### 3.1.n Fuente de información n sobre el tipo de tecnología en general

## 3.2 Fuentes sobre la tecnología Aircrack-NG

### 3.2.1 Fuente de información 1 sobre Aircrack-NG

Pagina web oficial de la herramienta Aircrack-NG. En su página web oficial, se ofrece todo tipo de documentación, tutoriales, videos, una wiki, el código fuente de la herramienta en github y mucha más información sobre la suite de Aircrack-NG.

Enlace: <https://www.aircrack-ng.org/documentation.html>

### 3.2.2 Fuente de información 2 sobre Aircrack-NG

La pagina web “Xataka.com” ofrece una guía de cómo usar la herramienta Aircrack-NG, con muchos detalles técnicos de lo que realmente hace la herramienta.

Enlace: <https://www.xataka.com/seguridad/caos-en-la-seguridad-wifi-un-repaso-a-las-vulnerabilidades-de-wep-wap-y-wap2>

### 3.2.3 Fuente de información 3 sobre Aircrack-NG

Es un documento PDF en el que varios profesores de la universidad central de Grecia explican los distintos protocolos de comunicaciones que existen en las redes de área local (WLAN) y como utilizar la herramienta Aicrack-NG para realizar ataques y explicar como funcionan dichos ataques.

Enlace: <https://pdfs.semanticscholar.org/7818/0b3c504fba41a000ac83c918c089c38f2eaf.pdf>

### 3.2.4 Fuente de información 4 sobre Aircrack-NG

Es un documento PDF en el que varios profesores de la universidad de Alabama en Huntsville y Frederick T. Sheldon del Oak Ridge National Laboratory, han escrito sobre los diferentes tipos de ataques que se pueden realizar a las redes Wifi de área local y como la herramienta Aircrack-NG dispone de los mecanismos para llevarlos a cabo.

Enlace: <http://eslared.net/walcs/walc2012/material/track4/Wireless/06193090.pdf>

### 3.2.5 Fuente de información 5 sobre Aircrack-NG

Es un documento PDF, el cual pues expuesto en el International Journal of Advanced Research in Computer Engineering & Technology, en el que se exponen varias manera de hacer expoiting con la herramienta Aircrack-NG en redes wifi con el sistema WPA (Wi-Fi Protected Access).

Enlace: <file:///C:/Users/Jorge/Downloads/wpaexplotationindworldofwirelessnetwork.pdf>

### 3.2.6 Fuente de información 6 sobre Aircrack-NG

Esta fuente es un documento PDF que podría dar apoyo a un curso de seguridad informática básica, en el que se explican muchos conceptos de seguridad. Entre estos conceptos, en el capitulo 8 “Ataques y contramedidas” hay un apartado dedicado a “Ataques Wi-Fi: Aircrack-NG” en el que se enseña como utilizar la herramienta Aircrack-NG.

Enlace: <https://s3.amazonaws.com/academia.edu.documents/34758985/Seguridad_Informatica_McGraw-Hill_2013_-_www.FreeLibros.me_-_copia.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1521373921&Signature=Oxt3JB9k%2F%2B1URaqPLZtrJHXmcW0%3D&response-content-disposition=inline%3B%20filename%3DSeguridad_Informatica_Mc_Graw-Hill_2013.pdf>

## 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

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

### 4.1.n Curso no gratuito n sobre el tipo de tecnología en general

## 4.2 Cursos no gratuitos sobre la tecnología Aircrack-NG

### 4.2.1 Curso no gratuito 1 sobre la tecnología Aircrack-NG

Este curso, es en modalidad online, lo imparten profesionales muy reconocidos en el mundo de la seguridad informática como son las personas que forman parte de la comunidad dragonjar. Ofrecen un contenido que se van actualizando constantemente. Entre esos contenidos se encuentra el de “Ataques actuales para redes inalámbricas” en el que se utiliza, entre otras, la herramienta Aircrack –NG.

El precio de este curso no es una cantidad en concreto, sino que es una suscripción anual de 1000 USD/año, por ello, los contenidos se van actualizando constantemente.

Enlace: <https://www.dragonjar.education/diplomado/>

### 4.2.2 Curso no gratuito 2 sobre la tecnología Aircrack-NG

En este online que se imparte gracias a la página web [www.pentestmag.com](http://www.pentestmag.com), se explica como hacer un test de seguridad en pentesting de redes Wi-Fi como un profesional. En el segundo modulo del curso, se estudia la herramienta Aircrack-NG.

Este curso no tiene un precio en concreto, sino que la pagina tiene la política de que cada usuario page una suscripción anual de 790 USD/año para que puedan acceder a los contenidos de este curso y de los demás cursos que imparten.

Enlace: <https://pentestmag.com/course/advanced-wireless-penetration-testing-15-2/>

### 4.2.3 Curso no gratuito 3 sobre la tecnología Aircrack-NG

Este curso lo imparte el Digital Tech Institute, está diseñado para empresas que quieran invertir en la formación de sus empleados y aumentar sus conocimientos en seguridad informática y hacking ético. En el módulo 4, de hacking ético, hay un apartado sobre ataques en redes inalámbricas, en el que se utilizara la herramienta Aircrack-NG.

Enlace: <http://www.digitaltechinstitute.com/formacion-in-company/itinerario-seguridad-it/#1484231461750-d6d95da4-788c>

4.2.4 Curso no gratuito 4 sobre la tecnología Aircrack-NG

En este curso se explican muchos conceptos sobre los protocolos y sistemas de las redes inalámbricas y como hacer tests de penetración en función de esos protocolos y sistemas. Para ello, entre otras herramientas, utilizan la herramienta Aircrack-NG.

Enlace: <https://backtrackacademy.com/curso/hacking-wireless>

## 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

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

### 5.1.n Curso gratuito n sobre el tipo de tecnología en general

## 5.2 Cursos gratuitos sobre la tecnología Aircrack-NG

### 5.2.1 Curso gratuito 1 sobre la tecnología Aircrack-NG

Este es un cuso que proporciona la web dragonjar, que es una comunidad hacker de latinoamerica muy reconocida en el mundo de la seguridad informática ofrece un curso gratuito de introducción a pentesting, en el que un apartado de su formación es “Ataques actuales para redes inalámbricas” en el que utilizan la herramienta Aircrack-NG.

Enlace: <https://www.dragonjar.education/curso/como-se-realiza-un-pentest/>

### 5.2.2 Curso gratuito 2 sobre la tecnología Aircrack-NG

En este curso están todos los tutoriales que los desarrolladores de la herramienta proveen a los usuarios. En este curso se enseña desde como instalar la herramienta a los distintos tipos de ataques que es capaz de levar a cabo Aircrack-NG. Ademas, estos tutoriales han sido traducidos a otros idiomas para ayudar a los usuarios con su comprensión.

Enlace: <https://www.aircrack-ng.org/doku.php?id=tutorial>

### 5.2.3 Curso gratuito 3 sobre la tecnología Aircrack-NG

Este es un curso que imparte la web [www.pkred.com](http://www.pkred.com) en el que le dedica un apartado al uso de la herramienta Aircrack-NG. En este curso, se enseña a utilizar la herramienta de una forma más avanzada y totalmente práctica.

Enlace: <https://pkred.com/publicaciones/Curso%20de%20Hacking%20Part%204.2%20::%20Claves%20Wifi,%20Aircrack-ng./595264d611f5ae34acd74bc5>

### 5.2.4 Curso gratuito 4 sobre la tecnología Aircrack-NG

Este es un curso gratuito sobre “Wireless penetration testing con Kali Linux” impartido totalmente en la plataforma Youtube por Marcos Mendoza, en el que enseña a utilizar diferentes herramientas de la distribución de software libre Kali Linux tiene para hacer test de penetración en redes Wi-Fi. Y una de esas herramientas es AirCrack-NG.

Enlace:

<https://www.youtube.com/playlist?list=PL-G03HRCQgdFKAaW718J14tKDM63mGirL>

## 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