



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

Comunicaciones WiFi seguras en entorno corporativo

Máster Universitario en Dirección TIC para la Defensa

ALUMNO: Juan Carlos Núñez García

DIRECTORES: Carlos Zamorano Pinal
Norberto Fernández García

CURSO ACADÉMICO: 2021-2022

Universida_{de}Vigo



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

Comunicaciones WiFi seguras en entorno corporativo

Máster Universitario en Dirección TIC para la Defensa
Especialidad de Sistemas y Tecnologías de Telecomunicación

UniversidadeVigo

RESUMEN

Desde los inicios de las redes inalámbricas (protocolo ALOHA, 1971) hasta la actualidad, las redes inalámbricas han evolucionado de manera notable. Hoy son el medio más común de acceso a Internet. No obstante, este tipo de redes no están exentas de riesgos, de hecho tienen casi todos los riesgos atribuibles a las redes cableadas más otro conjunto de riesgos propios de su condición de redes radiantes.

Para mejorar la seguridad de las redes de telecomunicaciones han surgido organizaciones que velan por que el despliegue y bastionado de las mismas sea la adecuada a la importancia de la información que por las mismas circula. En España es el Centro Criptológico Nacional es el organismo que vela por la seguridad de los sistemas de telecomunicaciones e información a través de la publicación de guías, llamadas CCN-STIC.

Este trabajo ha intentado mostrar el despliegue de una red WiFi en un organismo universitario de una forma segura y siempre bajo el punto de vista del Esquema Nacional de Seguridad, plasmado en las guías CCN-STIC.

Para el despliegue de la red se ha realizado un estudio del área de interés y de las atenuaciones que le podrían afectar como consecuencia de su distribución interior.

Asimismo, se ha valorado la información que circula por la red del estudio, estableciéndose el correspondiente nivel de seguridad, que ha motivado la posterior configuración de la red.

Por último, se han practicado una serie de pruebas con el objeto de valorar la eficacia de las medidas implementadas.

PALABRAS CLAVE

WiFi, Esquema Nacional de Seguridad, estándar, red inalámbrica.

AGRADECIMIENTOS

Para mi familia, que siempre me ha apoyado para la realización de este Master con paciencia y cariño.

Para mis compañeros, su compañerismo y buen hacer me han motivado para continuar y mejorar cada día.

Por supuesto, para mis tutores don Norberto y don Carlos, que me han guiado en este camino, a veces oscuro y tenebroso.

CONTENIDO

Contenido	1
Índice de Figuras	3
Índice de Tablas.....	6
1 Introducción y objetivos	7
1.1 Motivación	7
1.2 Objetivo.....	8
1.3 Metodología y estructura	8
2 Estado del arte	9
2.1 Redes inalámbricas 802.11	9
2.1.1 Historia de las redes inalámbricas	10
2.1.2 Ventajas, inconvenientes y clasificación de las redes inalámbricas	10
2.1.3 Componentes de las redes inalámbricas	12
2.2 Estandarización de las redes 802.11	14
2.2.1 Aspectos de seguridad del estándar 802.11	15
2.3 Estados de conexión de una red inalámbrica	18
2.4 Arquitectura WiFi de las redes corporativas	21
2.4.1 Topología de las redes WiFi	22
2.4.2 Arquitectura de las redes WiFi	23
2.4.2.1 Arquitectura lógica y física	23
2.4.2.2 Segregación de zonas, redes y roles	24
2.5 Riesgos, amenazas y ataques a redes WiFi	26
2.6 Esquema Nacional de Seguridad (ENS)	29
2.7 Software libre para la gestión de redes inalámbricas	30
3 Desarrollo del TFM	34
3.1 Descripción del proyecto	34
3.2 Propósito de la red inalámbrica.....	34
3.3 Uso adecuado de la red inalámbrica corporativa	35
3.4 Determinación del nivel de seguridad de la red corporativa.....	36
3.5 Requerimientos de seguridad de la red inalámbrica universitaria	37
3.5.1 Requerimientos técnicos	37
3.5.2 Requisitos operacionales	38
3.5.3 Requisitos de explotación	41
3.5.4 Requerimientos de Protección de Datos	43
3.6 Concepto y definición de la red a desplegar	44

3.7 Material empleado para el despliegue de la red inalámbrica	44
3.7.1 Descripción del punto de acceso.....	45
3.7.2 Configuración inicial del punto de acceso	48
3.7.3 Otro material necesario	56
3.8 Despliegue de la red	56
3.8.1 Estudio de la cobertura de la red.....	56
3.8.2 Valoración de opciones de despliegue	60
3.8.3 Despliegue de la red.....	62
3.8.4 Asignación direccionamiento IP	64
3.9 Bastionado de la Red WiFi.....	64
3.9.1 Control acceso de usuarios	67
3.9.2 Servidor de autenticación RADIUS	68
3.9.3 Configuración de la base de datos	70
3.9.4 Sistema de detección de intrusos	73
3.10 Acreditación de la red	78
4 Pruebas y valoración	79
4.1 Medidas complementarias y objetivos alcanzados	79
4.1.1 Nivel de seguridad	79
4.1.2 Cobertura del área.....	79
4.2 Valoración.....	80
4.2.1 Pruebas de penetración	80
5 Conclusiones y líneas futuras	85
5.1 Conclusiones	85
5.2 Líneas futuras	86
6 Bibliografía.....	87

ÍNDICE DE FIGURAS

Figura 2-1	Forma de clasificar las redes según su escala [10]
Figura 2-2	Tarjeta TCI [11]
Figura 2-3	Adaptador WiFi [12]
Figura 2-4	Adaptador PCMCIA [13]
Figura 2-5	Punto de Acceso TP. Link EAP115 [14]
Figura 2-6	Rúter inalámbrico Linksys WRT54G [15]
Figura 2-7	Antenas WiFi [16]
Figura 2-8	Actualizaciones del estándar 802.11 [19]
Figura 2-9	Protocolos de seguridad WiFi [29]
Figura 2-10	Modelo WPA2-Personal [30]
Figura 2-11	Modelo WPA2-Enterprise [30]
Figura 2-12	802.11 State Machine [32]
Figura 2-13	BSS y sus estaciones asociadas [33]
Figura 2-14	Diagrama de una red inalámbrica modo Ad Hoc [34]
Figura 2-15	Diagrama de una red inalámbrica modo infraestructura [34]
Figura 2-16	Arquitectura lógica de planos funcionales [34]
Figura 2-17	Arquitectura de interfaces físicas [34]
Figura 2-18	Segregación de zonas, redes y roles [34]
Figura 2-19	Interfaz usuario DD-WRT [51]
Figura 2-20	Interfaz usuario InSSIDer [54]
Figura 2-21	Interfaz usuario NetSpot [56]
Figura 3-1	Vista aérea de la ubicación de la instalación [73]
Figura 3-2	Categorización del Sistema “Universidad ENS” [61]
Figura 3-3	Área de interés (elaboración propia)
Figura 3-4	Esquema del concepto de la red a desplegar [30]
Figura 3-5	Guía CCN-STIC-105 Catálogo de productos TIC [69]
Figura 3-6	Vista exterior punto de acceso Ruckus R610 [71]
Figura 3-7	Patrones de radiación de la antena Ruckus R610 [71]
Figura 3-8	Esquema iluminación indicadores frontales Ruckus R610 [71]
Figura 3-9	Indicadores frontales Ruckus R610 [71]
Figura 3-10	Indicadores traseros Ruckus R610 [71]
Figura 3-11	Configuración por defecto del punto de acceso [71]

- Figura 3-12 Configuración por defecto del Access Point en el exterior del AP [71]
- Figura 3-13 Detalles de la conexión a red [97]
- Figura 3-14 Verificación ping IP 192.168.0.1 (elaboración propia)
- Figura 3-15 Consola de acceso web a la configuración del punto de acceso [97]
- Figura 3-16 Consola de administración del punto de acceso [97]
- Figura 3-17 Consola configuración del dispositivo [97]
- Figura 3-18 Configuración Internet [97]
- Figura 3-19 Configuración Radio 2,4G – Common [97]
- Figura 3-20 Configuración Wireless 1 y Wireless 2 [97]
- Figura 3-21 Configuración lista de acceso [97]
- Figura 3-22 Agregación MAC [97]
- Figura 3-23 Modos de funcionamiento del punto de acceso [97]
- Figura 3-24 Configuración cripto del punto de acceso [97]
- Figura 3-25 Configuración Hotspot [97]
- Figura 3-26 Configuración controlador y acceso al punto de acceso [97]
- Figura 3-27 Vista aérea de edificio propuesto de despliegue [73]
- Figura 3-28 Distribución interna del edificio (elaboración propia)
- Figura 3-29 Acrylic WiFi Heatmaps [76]
- Figura 3-30 Colocación de los Puntos de Acceso [76]
- Figura 3-31 Reducción de la potencia de emisión [76]
- Figura 3-32 Redes WiFi radiantes en la zona de interés [77]
- Figura 3-33 Saturación de canales en la banda de 2,4 Ghz [77]
- Figura 3-34 WDS (Wireless Distribution System) [79]
- Figura 3-35 Red mallada (MESH) [80]
- Figura 3-36 Diagrama de una red inalámbrica modo infraestructura [35]
- Figura 3-37 Diagrama de la instalación (elaboración propia)
- Figura 3-38 Diagrama de conexiones (elaboración propia)
- Figura 3-39 Acceso a la red de invitados [elaboración propia]
- Figura 3-40 Consola de PuTTY [98]
- Figura 3-41 Extracto superior consola de PuTTY [98]
- Figura 3-42 Extracto inferior consola de PuTTY [98]
- Figura 3-43 Acceso a credenciales PuTTY [98]
- Figura 3-44 Nuevo usuario servidor RADIUS (elaboración propia)
- Figura 3-45 Limitación de conexiones simultaneas (elaboración propia)

- Figura 3-46 Importación de tablas de RADIUS (elaboración propia)
- Figura 3-47 Tablas base datos MySQL (elaboración propia)
- Figura 3-48 Configuración radius.conf (elaboración propia)
- Figura 3-49 Configuración siter.available (elaboración propia)
- Figura 3-50 MySQL Enterprise Monitor [85]
- Figura 3-51 Arquitectura de un Sistema WIDS/WIPS [86]
- Figura 3-52 Actualización del repositorio opdk (elaboración propia)
- Figura 3-53 Instalación del dron Kismet (elaboración propia)
- Figura 3-54 Extracto de la carpeta /etc con el dron Kismet creado (elaboración propia)
- Figura 3-55 Configuración Drone Kismet (elaboración propia)
- Figura 3-56 Configuración Wireless 1 (elaboración propia)
- Figura 3-57 Arranque del servidor (elaboración propia)
- Figura 3-58 Consola Kismet en funcionamiento [90]
- Figura 3-59 Consola Kismet UI [59]
- Figura 3-60 Consola InSSIDer (elaboración propia)
- Figura 3-61 Suplantación MAC (elaboración propia)
- Figura 3-62 Consola Acceso SSH a través de PuTTY [98]
- Figura 3-63 Captura de credenciales SSH a través de Wireshark (elaboración propia)
- Figura 3-64 Interfaz de monitorización Wireless_1 (elaboración propia)
- Figura 3-65 aireplay-ng ejecuntandose (elaboración propia)
- Figura 3-66 Captura handshake (elaboración propia)
- Figura 3-67 Proceso de rotura de contraseña (elaboración propia)

ÍNDICE DE TABLAS

2-01	Guías CCN-STIC (elaboración propia)
2-02	Scanners (elaboración propia)
2-03	Sniffers (elaboración propia)
2-04	Crackers (elaboración propia)
3-01	Parámetros de configuración redes (elaboración propia)
3-02	Cuadro de conexiones (elaboración propia)
3-03	Direccionamiento IP (elaboración propia)
3-04	Configuración servidor RADIUS (elaboración propia)
3-05	Configuración específica servidor RADIUS (elaboración propia)
3-06	Configuración cliente RADIUS (elaboración propia)

1 INTRODUCCIÓN Y OBJETIVOS

1.1 Motivación

En plena era de la digitalización y en un mundo azotado por epidemias, pandemias, guerras y desastres naturales de todo tipo, la proliferación de dispositivos móviles y la mejora del ancho de banda de las conexiones inalámbricas a Internet han impactado de manera muy importante en la forma en que las organizaciones, empresas, empleados y clientes se relacionan entre sí.

Desde hace unos años, la proliferación masiva de tecnologías móviles basadas en teléfonos inteligentes ha posibilitado el uso masivo de Internet desde cualquier lugar y momento. Esta evolución tecnológica surgida en los años 70 del pasado siglo ha abierto también nuevas posibilidades en las organizaciones y empresas, posibilitando el acceso ágil y seguro de los empleados, clientes y proveedores a servicios de la empresa sin necesidad de complicados procedimientos de acceso o conexión a dichas redes. Así mismo, la presente pandemia ha relanzado un nuevo modo de trabajo seguro desde el propio domicilio, el teletrabajo, que posibilita mayor flexibilidad tanto para el empleado como para la empresa. Las conexiones inalámbricas también posibilitan el acceso a la red corporativa con seguridad, disponibilidad y agilidad desde puntos remotos en el caso de reuniones, viajes, etc.

Hoy en día el repertorio de tecnologías inalámbricas [01] disponibles para particulares y empresas es amplio. Aunque para el gran público en general la tecnología WiFi puede ser la más popular, existen otras más orientadas hacia usos más específicos, pero también basadas en conexiones inalámbricas, por ejemplo *ZigBee* [02] centrada en aplicaciones domóticas e industriales. *Bluetooth* [03] que permite la transmisión de datos a corto alcance y es también muy conocida dentro del ámbito de la electrónica de consumo. *Thread* [04] es una tecnología de red en malla de bajo consumo basada en IPv6 para IoT (*Internet of Things*) con diseño seguro y escalable y NFC (*Near Field Communication*) [05] permite la interacción segura entre dispositivos electrónicos, siendo especialmente adecuada para teléfonos inteligentes (*smartphones*), lo que la ha hecho muy popular.

La evolución y despliegue de las redes inalámbricas en nuestro día a día, están transformando la forma en que particulares, organizaciones, empresas, empleados y clientes se relacionan entre sí. Sin embargo, dichos avances también son una nueva fuente de riesgos a los que hay que hacer frente (pérdida o robo de información, robo de credenciales, robo de dispositivos, uso inadecuado de dispositivos móviles, uso de sistemas de conexión no seguros, etc.). En la medida en que la tecnología evolucione para proporcionar los recursos que los usuarios reclamen como la disponibilidad, confidencialidad, integridad y otros requerimientos de carácter técnico tales como velocidad de procesamiento, ancho de banda, acceso inmediato a

recursos en línea, marcará el ritmo hacia un progresivo abandono de redes fijas hacia redes inalámbricas debido a las indudables ventajas que estas últimas proporcionan, aunque también supongan una fuente inagotable de problemas de seguridad.

1.2 Objetivo

El objetivo principal con este trabajo es elaborar un documento técnico que permita a una organización bajo el paraguas del Esquema Nacional de Seguridad (ENS) [06, 45] establecer un modelo de arquitectura de referencia para la implementación de un sistema de comunicaciones móviles seguro basado en el estándar general 802.11ac (WiFi) en un entorno corporativo, así como la configuración segura de la misma, con la suficiente flexibilidad para que sea posible:

- Determinar el nivel de seguridad adecuado a la red corporativa a instalar.
- Gestionar la documentación categorizada según el Esquema Nacional de Seguridad.
- Permitir el envío seguro de información entre los dispositivos de los empleados.
- Permitir la salida de información hacia redes cableadas permanentes.
- Gestionar y configurar los principales elementos físicos y lógicos que forman parte de una infraestructura de red inalámbrica.
- Dotar a todo el espacio físico de interés de cobertura WiFi de calidad.
- Dotar a la red inalámbrica de las medidas de seguridad que establece el Esquema Nacional de Seguridad, en relación a la información que se maneja.
- Proporcionar una red de invitados.

En definitiva, el trabajo tratará de establecer un conjunto de directrices, pautas y guías para implementar un sistema de comunicaciones móviles seguro basado en el estándar general 802.11ac (WiFi) en un entorno corporativo.

1.3 Metodología y estructura

La metodología empleada va en línea con los objetivos indicados en el punto anterior. Los diferentes pasos se detallan a continuación:

- En el estado del arte se abordará la historia de las redes inalámbricas, se repasará el proceso de estandarización de la tecnología basada en el estándar 802.11. Se analizarán los estados de conexión a una red inalámbrica, la arquitectura del servicio WiFi a redes corporativas, las amenazas a la seguridad en una red WiFi, estandarización de las redes WiFi, se repasarán algunos conceptos del Esquema Nacional de Seguridad (ENS) [06, 45] y por último se mostrarán algunos ejemplos de software libre para la gestión y monitorización de redes inalámbricas. El objetivo es aprender y entender como actualmente abordan las organizaciones los beneficios y riesgos del empleo de esta tecnología.
- Con la información recopilada en el punto anterior se afrontará el diseño de una arquitectura de referencia para la implantación de un sistema de comunicaciones inalámbricas seguro basado en el estándar 802.11ac. Realizándose un estudio del área de interés, de los elementos físicos necesarios para su materialización y de la configuración de los mismos. Así mismo, se determinará el nivel de seguridad necesario según el Esquema Nacional de Seguridad y las medidas de seguridad necesarias para su implantación.
- Se llevará a cabo una validación de los requisitos de seguridad del diseño, en el cual se revisará que se han cubierto satisfactoriamente todos los riesgos identificados con las correspondientes salvaguardas de seguridad.
- Por último, se extraerán las conclusiones correspondientes del trabajo realizado y se propondrá mejoras o aspectos a considerar en el futuro.

2 ESTADO DEL ARTE

En el capítulo del estado del arte, se intentará plasmar la base teórica sobre que la se sustentará el desarrollo del TFM que se acometerá con posterioridad.

2.1 Redes inalámbricas 802.11

2.1.1 Historia de las redes inalámbricas

Desde el inicio de la era de la computación [08] los usuarios de esos primitivos sistemas soñaban con entrar en sus oficinas (usar computadoras en el domicilio era ciencia ficción) y que sus ordenadores portátiles se conectaran “*mágicamente*” con una red externa que les proporcionase una fuente de información adicional. En consecuencia, varios grupos de investigadores comenzaron a trabajar y dar los primeros pasos con el objetivo de hacer realidad dicha “*magia*” y que llegase a lo que actualmente conocemos como Internet.

En un principio la metodología más práctica consistía en dotar a los dispositivos de pequeños emisores y receptores radio de corto alcance para que la comunicación pudiese existir. Así mismo, se precisaba un receptor fijo para recoger dicha señal de los terminales móviles e integrarla en la red fija.

En 1971 un grupo de investigadores bajo la dirección del Norman Abramson, en la Universidad de Hawái, crearon el primer sistema de conmutación de paquetes mediante una red de comunicación por radio, dicha red se llamó ALOHA [07]. Esta fue la primera red de área de área local inalámbrica. Estaba formada por 7 estaciones situadas cada una en una isla diferente y que se podían comunicar a través de una estación central.

Estos trabajos rápidamente dieron sus primeros frutos y varias empresas comenzaron a ofrecer productos basados en redes LAN (*Local Area Network*) inalámbricas. En un principio estas redes inalámbricas ofrecían un mecanismo basado en la empresa que la había creado, motivo por el cual un dispositivo de la empresa/marca “A” no podía comunicarse con otro dispositivo de la empresa/marca “B” debido a que sus estándares eran diferentes. Pronto se hizo necesaria la estandarización de tecnologías, de modo que el comité del IEEE (*Institute Electrical and Electronic Engineers*) que ya había estandarizado las redes cableadas recibió la tarea de idear un estándar para las nuevas redes inalámbricas.

La primera decisión del IEEE fue la de denominar a este nuevo estándar. Los anteriores estándares se denominaban con los números 802.1, 802.2 hasta el 802.10, así que la siguiente nomenclatura lógica sería la 802.11.

Coloquialmente al estándar IEEE 802.11 se le conoce como WiFi. Hay varias teorías de como el estándar 802.11 se pasó a llamar WiFi. Una de ellas es pensar que el término deriva de

una similitud con HiFi (*High Fidelity*), un concepto de moda en el momento que se implementó el estándar 802.11, representado por el acrónimo WiFi (*Wireless Fidelity*). Sin embargo, en el año 2005 Phil Belanger, uno de los miembros fundadores del WiFi Alliance, reveló que el nombre sólo era una estrategia de mercado. Ninguna de las opciones anteriores está totalmente confirmada, dependiendo de la fuente puede ser una u otra opción.

Obviamente en estos primeros pasos de este estándar se tuvieron que acometer retos de alto nivel. El primero fue hallar una banda de frecuencia adecuada que estuviese disponible, si era posible, a nivel mundial. Se descartó el uso de bandas de frecuencias bajo licencia que eran costosas, y se optó por bandas sin licencia como las ISM (*Industrial, Scientific and Medical*) definidas por el ITU-R (*International Telecommunication Union – Radio*), por ejemplo las bandas de 902-929 MHz, 2,4-2,6 GHz y 5,725-5,825 GHz [91]. Cualquier dispositivo tendría la posibilidad de usar dichas bandas con la única limitación de la potencia de emisión que debería ser la mínima imprescindible para garantizar la comunicación.

2.1.2 Ventajas, inconvenientes y clasificación de las redes inalámbricas

Mucho se ha escrito en relación a las ventajas e inconvenientes de las redes inalámbricas en comparación con las redes cableadas, a continuación se citan algunas de las ventajas e inconvenientes más evidentes de las redes inalámbricas:

Las ventajas más sobresalientes de usar redes inalámbricas podrían ser [08]:

- Facilidad y rapidez de instalación.
- Movilidad: La libertad de movimientos es una de las ventajas más evidentes de este tipo de redes.
- Flexibilidad: Adaptación con facilidad a las circunstancias diversas.
- Escalabilidad: Facilidad de expandir la red después de su instalación inicial.
- Ahorro de costes: Abaratamiento y facilidad de implantación y bajo coste de los dispositivos necesarios para su puesta en funcionamiento.

No obstante, también tienen desventajas:

- Velocidad limitada en relación a las velocidades de las redes cableadas.
- Mayor inseguridad que las redes cableadas: El área de expansión de la red puede abarcar espacios no controlados y por tanto vulnerables.
- Interferencias: Las redes WiFi funcionan entre otras en las bandas de 2,4 GHz y 5 GHz. Esta banda no requiere licencia administrativa por lo que es ampliamente usada en el mercado y por tanto una fuente de interferencias (por ejemplo: hornos microondas).
- Alcance: Determinado por la potencia de los puntos de acceso y en constante equilibrio con la seguridad. En principio a mayor potencia de emisión mejor señal llegaría a los usuarios y por lo tanto mayor calidad de señal recibirían estos. Sin embargo, el exceso de potencia de radiación supone que la señal puede desbordar nuestras instalaciones y suponer una vulnerabilidad.

Respecto a la seguridad y como introducción a lo que posteriormente se convertirá en una parte sustancial de este trabajo, hay que señalar que se ha realizado un gran esfuerzo en mejorar la seguridad de las redes inalámbricas, implementando diferentes protocolos y métodos de protección a lo largo de la corta historia de dichas redes. En este proceso de bastionado de las redes inalámbricas se han sucedido diferentes métodos, como por ejemplo la restricción de direcciones MAC (*Media Access Control*), y la implementación de sucesivos protocolos que han

evolucionado al ritmo que han impuesto las propias debilidades, por ejemplo del protocolo WEP (*Wired Equivalent Privacy*) [08].

Podemos clasificar a las redes en cinco tipos de menor a mayor escala, tal y como se muestra en la figura 2-1:

- **Redes PAN** (*Personal Area Network*): Son redes que comunican los dispositivos muy cercanos de un usuario. El ejemplo más actual podría ser el *Bluetooth*.
- **Redes LAN** (*Local Área Network*): Son redes de área local que pueden englobar desde una vivienda a un edificio. Su objetivo es compartir información y recursos entre los equipos pertenecientes a la LAN. En el caso de las redes inalámbricas tipo WiFi se basan en el estándar IEEE 802.11.
- **Redes MAN** (*Metropolitan Área Network*): Pueden abarcar una ciudad. Surgieron por la necesidad de dar cobertura de TV dentro de las ciudades. Actualmente existe la tecnología *WIMAX*, estándar IEEE 802.16 [09] que permite la creación de redes MAN en las áreas metropolitanas de forma inalámbrica.
- **Redes WAN** (*Wide Área Network*): Abarcan una amplia cobertura geográfica, por ejemplo un país o un continente. Diferencian a los usuarios y a las subredes que a su vez suelen estar gestionadas por grandes ISP (*Internet Service Provider*).
- **Interredes**: Son conjunto extenso de redes interconectadas. Por ejemplo, Internet.

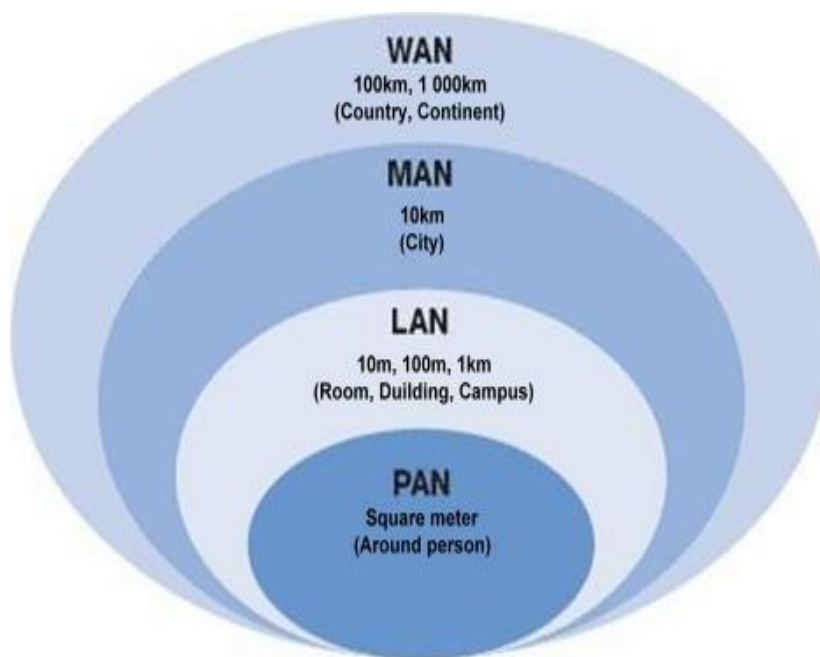


Figura 2-1 Forma de clasificar las redes según su escala [10]

Existen otras muchas maneras de clasificar las redes de comunicaciones, por ejemplo la clasificación por su topología, por el método de conexión, por su relación funcional, por la direccionalidad de los datos, por su rango de frecuencias, etc. No obstante, este trabajo se centrará en las redes inalámbricas, más concretamente en las redes de área local inalámbricas o WLAN (*Wireless Local Area Network*) basadas en el estándar IEEE 802.11.

Las redes WiFi están compuestas por los clientes, que pueden ser teléfonos móviles, ordenadores portátiles u otros dispositivos, y por una infraestructura que consiste en puntos de acceso o estaciones base, que son fijas y normalmente se instalan en edificios. Estos puntos de acceso se conectan a la red cableada proporcionando los servicios que existen en la misma.

2.1.3 Componentes de las redes inalámbricas

Hoy en día existen innumerables dispositivos que nos proporcionan acceso a las redes inalámbricas. Según avanza la tecnología muchos dispositivos se integran en otros e incluso desaparecen para dar paso a otros más avanzados y con mejores prestaciones. No obstante, a continuación se citan los principales dispositivos inalámbricos necesarios para la instalación y configuración de una red de este tipo:

- **Tarjeta PCI** (*Periphertral Component Interconnect*):

Sirve para enviar y recibir datos sin necesidad de cables. Usan una ranura PCI para conectarse al PC (figura 2-2). Hoy en día gran parte de los dispositivos traen integradas este tipo de tarjetas. No obstante, los dispositivos precisan de una tarjeta (*Network Interface Card*) que puede estar integrada en el dispositivo o externa con distintas posibilidades de interconexión.



Figura 2-2 Tarjeta PCI [11]

- **Adaptador USB-WiFi:**

Se emplean ampliamente debido a su comodidad y versatilidad de instalación. Existen múltiples modelos a diversos precios (figura 2-3).



Figura 2-3 Adaptador WiFi [12]

- **Adaptador PCMCIA WiFi:**

Los adaptadores PCMCIA (*Personal Computer Memory Card International Association*) están diseñados para el funcionamiento en ordenadores portátiles. Hoy en día prácticamente todos los dispositivos portátiles traen este adaptador integrado de fábrica (figura 2-4).



Figura 2-4 Adaptador PCMCIA [13]

- Punto de Acceso:

Es el dispositivo (figura 2-5) que interconecta los equipos de la red inalámbrica. Normalmente se conecta a su vez a una red cableada para interconectar ambas redes. Los puntos de acceso pueden interconectarse entre sí y de esta forma ampliar el área de cobertura de la red.



Figura 2-5 Punto de Acceso TP. Link EAP115 [14]

Los puntos de acceso tienen dos características fundamentales:

- Potencia de transmisión: Se mide en dBm o mw (miliwatts).
- Sensibilidad del receptor: Se refiere a la potencia mínima de las señales que pueden ser detectadas por el equipo. Se mide en dBm.

Los puntos de acceso hardware pueden ofrecer múltiples servicios tales como servidor DHCP (*Dynamic Host Configuration Protocol*), filtrado de direcciones MAC, cifrado, etc.

- Enrutador Inalámbrico:

Es el encargado de conectarnos a una red exterior (p.ej.: Internet) normalmente a través de la red de nuestro ISP (figura 2-6).

Puede realizar las funciones adicionales de filtrado de páginas web, control de acceso de usuarios, horarios, etc.



Figura 2-6 Rúter Inalámbrico Linksys WRT54G [15]

- Antenas:

La antena (figura 2-7) es el elemento radiante de la red, pueden existir varios tipos:

- Direccional: Tiene un haz estrecho y de largo alcance.

- Omnidireccional: Tiene un haz amplio y de corto alcance.
- Sectorial: Son una mezcla entre las antenas direccionales y omnidireccionales, intentando el balancear sus ventajas e inconvenientes.



Figura 2-7 Antenas WiFi [16]

2.2 Estandarización de las redes 802.11

Como ya se ha comentado en el punto anterior, el IEEE es un organismo internacional encargado de la estandarización de productos relacionados con la electricidad y la electrónica. No obstante, es una de las mayores organizaciones técnicas y profesionales dedicadas al avance de la tecnología. Entre sus funciones está la innovación y la excelencia de los productos que estandariza y promociona [17].

La Real Academia de la Lengua española, define el término estándar como “*Que sirve como tipo, modelo, norma, patrón o referencia*” [18]. El término fue españolizado del término inglés “*standar*” y se ajusta con plenitud a las misiones del IEEE que se encarga de la creación de normas y reglas para la fabricación y uso de diferentes tipos de tecnología, desde la instrumentación, ingeniería, ultrasonidos, etc. [17]. Este trabajo se centrará en su aspecto en redes inalámbricas, por lo tanto el estándar adecuado, como anteriormente ya se ha comentado es el 802.11.

El estándar 802.11 ha sufrido sucesivas revisiones y actualizaciones desde su primera versión en 1997 hasta nuestros días (figura 2-8). IEEE es una organización que estandariza a nivel mundial, pero eso no quiere decir que sus revisiones y actualizaciones se apliquen de forma inmediata en todas las partes del mundo, ya que dicha implantación depende de que los dispositivos a los que va dirigido soporten dichas actualizaciones. Por lo tanto, las actualizaciones del estándar 802.11 que el IEEE publica pueden tardar años en estar plenamente vigentes en los dispositivos clientes, incluidas las recomendaciones de seguridad.

A continuación se muestran algunas de las revisiones y actualizaciones del estándar 802.11 a lo largo del tiempo.

IEEE Standard	Year Adopted	Frequency	Max. Data Rate	Max. Range
802.11a	1999	5 GHz	54 Mbps	400 ft.
802.11b	1999	2.4 GHz	11 Mbps	450 ft.
802.11g	2003	2.4 GHz	54 Mbps	450 ft.
802.11n	2009	2.4/5 GHz	600 Mbps	825 ft.
802.11ac	2014	5 GHz	1 Gbps	1,000 ft.
802.11ac Wave 2	2015	5 GHz	3.47 Gbps	10 m.
802.11ad	2016	60 GHz	7 Gbps	30 ft.
802.11af	2014	2.4/5 GHz	26.7 Mbps – 568.9 Mbps (depending on channel)	1,000 m.
802.11ah	2016	2.4/5 GHz	347 Mbps	1,000 m.
802.11ax	2019 (expected)	2.4/5 GHz	10 Gbps	1,000 ft.
802.11ay	late 2019 (expected)	60 GHz	100 Gbps	300-500 m.
802.11az	2021 (expected)	60 GHz	Device tracking refresh rate 0.1-0.5 Hz	Accuracy <1m to <0.1m

Figura 2-8 Actualizaciones del estándar 802.11 [19]

2.2.1 Aspectos de seguridad del estándar 802.11

La primera versión del estándar IEEE 802.11 [20] para conexiones inalámbricas se ratificó en el año 1997, en dicho estándar se incluyó el apartado de seguridad basado en *Wired Equivalent Privacy* (WEP). En dicho algoritmo de seguridad se creó para dotar de seguridad a las redes inalámbricas de la misma manera que se dotaba a las redes cableadas.

El protocolo WEP hace uso del mecanismo CRC-32 para garantizar su integridad, y del cifrado RC4 de 64 bits con una clave de 40 bits que se concatenaba a un vector de iniciación (IV) de 24 bits para conformar la clave. Al usuario se le mostraba como un conjunto de 10 caracteres hexadecimales (números del 0 al 9 y letras de la A a la F).

El protocolo WEP mostró su debilidad en 2001 cuando unos investigadores (Scott R. Fluher, Isik Mantin y Adi Shamir) publicaron una investigación [20] sobre los problemas del cifrado RC4 y demostraban de una manera sencilla cómo descifrar dichas claves en un tiempo reducido espionando las comunicaciones y analizando los paquetes que se intercambiaban entre el cliente y el punto de acceso. De hecho, en el caso de que existiese un tráfico escaso, era posible estimular la respuesta del punto de acceso y lograr la cantidad suficiente de vectores de iniciación IV para descifrar la clave WEP.

Esta debilidad del RC4 invalidó al protocolo WEP como un protocolo seguro y pronto se volvió uno de los ataques clásicos a este tipo de redes. Herramientas como “Aircrack-ng” pronto permitió atacar y conseguir el acceso a una red WiFi en cuestión de minutos.

En contra de toda lógica muchas operadoras mantuvieron durante bastante tiempo el protocolo WEP como protocolo de seguridad por defecto en sus puntos de acceso. Curiosamente el detonante que supuso la defunción definitiva del protocolo WEP fue la brecha de seguridad basada en este protocolo de RJ Maxx, una de las mayores empresas comerciales de EE.UU, a la cual un atacante llamado Albert González robo 100 millones de cuentas de usuario y supuso unas pérdidas cercanas a 1.000 millones de dólares [21]. A partir de este incidente la industria tecnológica, las compañías suministradoras y los usuarios tomaron conciencia del riesgo y se comenzó a dejar de usar la tecnología basada en el protocolo WEP. No obstante, algunas compañías suministradoras de servicios inalámbricos intentaron parchear el problema con claves más largas y robustas o con pequeñas variaciones del protocolo WEP, como por ejemplo el WEP2 o WEPplus, sin embargo, dichos intentos tuvieron poco éxito ya que la debilidad era inherente al protocolo WEP.

El protocolo WPA (*Wi-Fi Protected Access*) surgió con la condición inicial de que fuese aplicable a los dispositivos existentes como una actualización del firmware en los enrutadores y demás equipos de comunicaciones, criterio que se ha mantenido para protocolos posteriores. Esto evitó el cambio total de la infraestructura ya existente. No obstante, resultó que algunos puntos de acceso antiguos necesitaban contar con requisitos adicionales que en muchos casos no podían satisfacer, por lo tanto hubo gran cantidad de puntos de acceso que no fueron actualizados y siguieron siendo vulnerables.

Con WPA la clave se cambiaba por cada paquete, con lo que se evitaba que fuese inmune al mismo ataque que el protocolo WEP. El protocolo WPA también incluía al protocolo (*Temporal Key Integrity Protocol*) como solución temporal y fallida para minimizar las vulnerabilidades del protocolo WPA basada en la reutilización de la clave WEP.

No obstante, de nuevo se vio que aquel esfuerzo no era suficiente. Martin Beck, creador de aircrack-ng y Erik Tews demostraron en 2008 [22, 23] que eran factibles ataques contra TKIP a través de la vulnerabilidad Chopchop (el atacante inyecta paquetes sin conocer la clave y espera a obtener la respuesta del punto de acceso para descifrar el resultado). Poco después aparecieron más estudios y variaciones de código que lograban inyectar paquetes y descifrarlos con el objeto de secuestrar la sesión e inyectar código malicioso.

En 2004 surgió otro protocolo que por fin “aseguraría” las conexiones WiFi contra todo tipo de ataque: el protocolo WPA2 [24], una nueva versión del protocolo WPA, que en realidad era una nueva implementación del estándar 802.11i.

WPA2 sustituye tanto al protocolo TKIP como al cifrado RC4 que se usaba en los protocolos WEP y WPA. WPA2 usa el cifrado *Advanced Encryption Standard* (AES) y el llamado “*Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*” (CCMP) [25].

El protocolo WPA2 ha demostrado ser mucho más robusto ante ataques que sus anteriores predecesores, aunque no ha sido inmune a otro tipo de ataques, por ejemplo a la vulnerabilidad llamada Hole196 [26]. Otro problema del protocolo WPA2 es el uso de contraseñas débiles, fácilmente descifrables mediante ataques de fuerza bruta y mediante el uso alternativo de ingeniería social para lograr que el usuario proporcione su contraseña.

Por lo tanto, las contraseñas son el talón de Aquiles tanto del protocolo WPA como del protocolo WPA2. Aunque los fabricantes de equipos de comunicaciones (enrutadores, puntos de acceso, etc.) establecían contraseñas relativamente robustas para proteger sus equipos, los usuarios por comodidad solían cambiarlas por otras más sencillas y fáciles de recordar. Estas segundas contraseñas serían un verdadero problema para las redes WiFi, especialmente las redes residenciales, debido a que eran fácilmente descubiertas a través de fuerza bruta con diccionario.

Otro problema que encontraba el usuario medio era lo costoso e incómodo que era conectar cierto tipo de dispositivos al punto de acceso. Para resolver este problema surgió el *WiFi Protected Setup* (WPS), coloquialmente llamado “botón azul”. La idea era realmente buena, con solo apretar un botón ambos equipos (cliente y punto de acceso) se sincronizaban y conectaban con una mínima intervención del usuario. Sin embargo, WPS supuso otro motivo de preocupación para las redes con protocolo WPA y WPA2. Pronto se descubrió que WPS estaba expuesto a un ataque que permitía conseguir la clave WiFi sin necesidad de diccionario. Finalmente se recomendó desactivar la opción WPS de los enrutadores, de nuevo esta recomendación tardó tiempo en implantarse totalmente dejando innumerables enrutadores en un estado de vulnerabilidad.

En 2018 WiFi Alliance anunció el lanzamiento del último estándar llamado WPA3 (Acceso WiFi Protegido 3) [27] sucesor del estándar WPA2. Como hemos visto anteriormente, las contraseñas y su fortaleza son un gran problema en la seguridad WiFi. Por lo tanto, el estándar WPA3 trata de prevenir y corregir dicha vulnerabilidad evitando el uso de contraseñas compartidas. WPA3 registra a los usuarios a través de un nuevo sistema llamado *WiFi Device Provisioning Protocol* (DPP) que no tiene clave compartida.

Con DPP, las redes utilizan códigos QR (*Quick Response*) o etiquetas NFC (*Near Field Communications*) para permitir que los usuarios accedan a la red. Al tomar una imagen o recibir una señal de radio del enrutador, el dispositivo puede ser autenticado sin comprometer la seguridad.

La encriptación WPA3 descarta mecanismos de cifrado antiguos y comprometidos en favor de otros protocolos de encriptación aún no vulnerados. El protocolo utilizado por WPA3 es el protocolo *Galois/Counter Mode Protocol* (GCMP-256) [28] de 256 bits, lo que refuerza el cifrado de WPA3.

Como resumen a lo anteriormente expuesto se añade un cuadro esquemático (figura 2-09) [29]:

	WEP	WPA	WPA2	WPA3
Brief description	Ensure wired-like privacy in wireless	Based on 802.11i without requirement for new hardware	All mandatory 802.11i features and a new hardware	Announced by Wi-Fi Alliance
Encryption	RC4	TKIP + RC4	CCMP/AES	GCMP-256
Authentication	WEP-Open WEP-Shared	WPA-PSK WPA-Enterprise	WPA2-Personal WPA2-Enterprise	WPA3-Personal WPA3-Enterprise
Data integrity	CRC-32	MIC algorithm	Cipher Block Chaining Message Authentication Code (based on AES)	256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256)
Key management	none	4-way handshake	4-way handshake	Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA)

Figura 2-9 Protocolos de seguridad WiFi [20]

Dentro de los protocolos WPA/WPA2/WPA3 existe la posibilidad de configurar el acceso a través de dos modos WPA-Personal o WPA-Enterprise [30], vamos a ver sus principales diferencias:

- **WPA2-Personal:** (figura 2-10) Proporciona seguridad para hogares y pequeñas redes de oficina. La mayoría de los enrutadores actualmente ofrecen esta opción y supone una protección relativamente eficaz ante ataques.

El principal problema de WPA2-Personal reside en que depende de una clave compartida entre todos los usuarios y dispositivos de red. Con lo que un hipotético atacante podría fácilmente hacerse con dicha clave y usarla para acceder a la red. En un entorno residencial este tipo de seguridad puede ser suficiente pero en un entorno empresarial/corporativo este tipo de seguridad puede acarrear grandes riesgos.

- **WPA2-Enterprise:** (figura 2-11) Supone un grado mayor de sofisticación a la hora de configurar la red. Se requiere un servidor de autenticación tipo RADIUS (o equivalente), el cual hace uso de una base de datos con los datos de las credenciales de los clientes. Con esta modalidad se mejora el rastreo, administración, manipulación de datos y proporciona al administrador de la red la posibilidad de deshabilitar fácilmente una cuenta de usuario en caso de ser necesario. Normalmente, un usuario necesita la credencial de cliente así como un proceso de autenticación. No obstante, podemos incluir un certificado digital para el acceso a zonas de la red que deban tener más protección o bien a toda la red en caso de que se quiera mejorar la seguridad en su conjunto. En este último caso, el usuario necesita la credencial de usuario y contraseña y el certificado digital para acceder a la red, por lo tanto se proporciona un mayor nivel de seguridad ante ataques.

En muchas empresas, podemos también encontrar un servidor Microsoft Windows con Directorio Activo. Este sistema es muy utilizado actualmente para la gestión de usuarios en una red corporativa y nos permite vincular un servidor RADIUS para la mejor gestión de usuarios, llevar un registro de los accesos a la red, nivel de privilegios, niveles de acceso y personalización de clientes, etc.



Figura 2-10 Modelo WPA2-Personal [30]



Figura 2-11 Modelo WPA2-Enterprise [30]

2.3. Estados de conexión a una red inalámbrica

Desde el momento en que seleccionamos la red inalámbrica con la cual deseamos conectarnos hasta el momento en que la conexión se realiza con éxito, el dispositivo debe de pasar por una serie de estados intermedios [31]:

- Estado 1: Estado inicial, no autenticado ni asociado.
- Estado 2: Autenticado, no asociado.
- Estado 3: Autenticado y asociado, aunque pendiente de la autenticación RSN (*Robust Security Network*).
- Estado 4: Autenticado y asociado. El terminal puede hacer uso de la red.

Cuando el dispositivo haya completado progresiva y exitosamente cada una de las cuatro fases, nuestro dispositivo no solo habrá establecido una asociación con el punto de acceso, sino que más importante aún, el punto de acceso le permitirá pasar tráfico a través de él.

A continuación, se intentará esquematizar la figura 2-12 centrándose en los detalles importantes y en la transición de un estado a otro:

- **Estado 1 Estado inicial, no autenticado ni asociado:** Este es el estado inicial del proceso, el cliente no está ni autenticado ni asociado, por lo tanto no está en absoluto conectado con la red inalámbrica y simplemente se realiza el proceso de escaneo pasivo y activo, descubriendo redes a su alrededor. Para superar esta fase el cliente debe completar exitosamente lo que se conoce como “autenticación 802.11”.
- **Estado 2 Autenticado, no asociado:** Se refiere a una autenticación tipo usuario y clave de acceso que seguramente es la primera opción que se piensa cuando se escuchar la

palabra autenticación. En realidad esta autenticación consiste simplemente en un “saludo” entre ambos dispositivos (cliente y el punto de acceso), con el objetivo de ratificar que ambos dispositivos son compatibles.

Para pasar del Estado 2 al Estado 3, el cliente debe completar exitosamente el proceso de asociación con el punto de acceso.

- **Estado 3 Autenticado y asociado:** Aunque pendiente de la autenticación RSN. Al inicio de este estado el cliente solicita al punto de acceso permiso para unirse y ser parte de su BSS (*Basic Service Set*). Un BSS consiste en un punto de acceso con varias estaciones clientes comunicándose a través de dicha BSS. Las estaciones clientes se conectan con la BSS, a nivel de capa 2 (figura 2-13).

Los cuatros estados se definen en el diagrama conocido como “802.11 State Machine”, que se muestra a continuación en la figura 2-12:

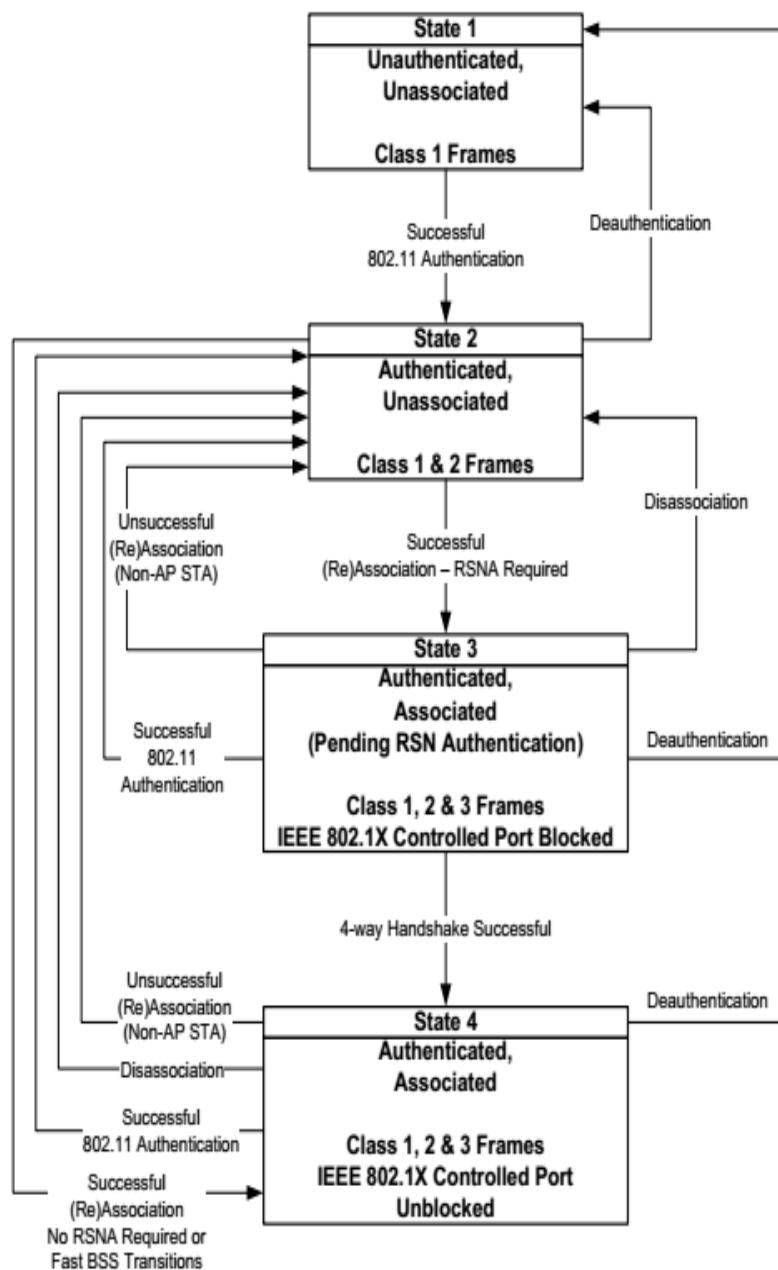


Figura 2-12, 802.11 State Machine [32]

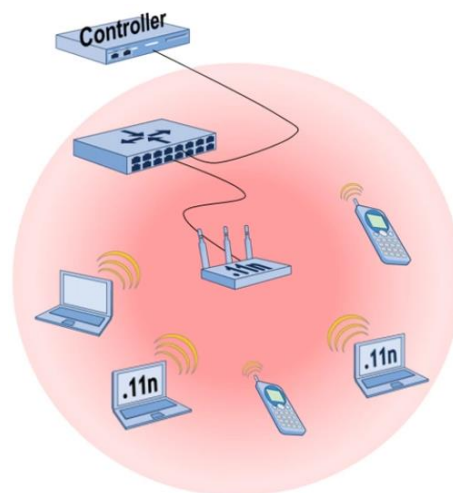


Figura 2-13 BSS y sus estaciones asociadas [33]

La asociación es también bastante simple y consiste en el intercambio de un par de mensajes “request” y “response”:

- La estación cliente envía un mensaje “*Association Request*” al punto de acceso y este le confirma su recepción devolviendo un “*Acknowledge*”.
- A continuación, el punto de acceso envía un mensaje de “*Association Response*” al cliente y esta confirma su recepción a través de un “*Acknowledge*”.
- Cuando se logra la asociación exitosa del cliente con el punto de acceso este último envía dentro del mensaje de respuesta “*Association Response*” un parámetro llamado “*Association ID*”. Este identificador es el número de asociación del cliente, es un identificador único que el punto de acceso entrega a cada cliente asociado exitosamente.

En este punto el cliente está autenticado y asociado, pero aún queda por completar los mecanismos de seguridad adicionales requeridos para redes con seguridad robusta.

- **Estado 4 Autenticado y asociado:** El paso de la fase 3 a la 4 involucra un proceso conocido como “4-way Handshake” que generará las claves de encriptación dinámicas que tanto el cliente como el punto de acceso emplearán para encriptar/desencriptar las tramas de datos.

Los pasos adicionales de seguridad son los siguientes:

- Autenticación: A través de los protocolos 802.1X/EAP (*Extensible Authentication Protocol*), WPA2-Enterprise/Personal o PSK (*Pre-shared keys*).
- Creación de clave maestra (*Master Key Creation*): Generación de las claves PMK/GMK (*Pairwise Master Key/Group Master Key*).
- Creación de clave temporal (*Temporal Key Creation*): Usando 4-way Handshake se generan las claves PTK/GTK (*Pairwise Transient Key/Group Temporal Key*).
- Autorización: En este punto se desbloquea el puerto controlado en el punto de acceso y este permite el tráfico de datos a través de la red.
- Encriptación: El tráfico de datos 802.11 es cifrado empleando como base las claves PTK/GTK.

Por último, se podría definir una 5ª fase que sería la correspondiente a la finalización de la conexión del cliente. Esta fase contempla la pérdida de la asociación entre el punto de acceso y el

cliente. El punto de acceso desautoriza al cliente, se eliminan las claves empleadas y el puerto previamente abierto vuelve a bloquearse, impidiendo el tráfico de datos.

Como resumen, hemos visto que estos procesos participan dos actores principales:

- **Cliente:** Es cualquier dispositivo de usuario que solicita al punto de acceso interactuar con la red inalámbrica para realizar transferencias de datos.
- **Punto de Acceso:** Son los puntos, normalmente fijos, que permiten conectar a los usuarios móviles a la red fija, otros puntos de acceso u otros usuarios móviles.

A estos dos elementos habría que añadirles uno que los complementa, el servidor de autenticación. Estos servidores son los encargados de gestionar el acceso de clientes a la red y la expedición de certificados. Para que un cliente alcance a un servidor de autenticación, previamente ha tenido que afrontar y superar exitosamente los cuatro estados de conexión. Una vez superados dichos estados, el punto de acceso permite al cliente el acceso a la red y pasa directamente al servidor de autenticación que gestiona las cuentas de usuario credenciales y privilegios de los mismos. Dicho servidor también gestiona una base de datos con las credenciales de acceso de cada usuario.

Los puntos de acceso se pueden configurar para distintas funciones para adaptarlos a las necesidades de la red. Estas son algunas de las funciones:

- **Modo Cliente:** El punto de acceso se comporta como un receptor y actuando como si fuese un cliente conectado a través de cable con la red.
- **Modo Punto de Acceso:** El punto de acceso sirve de núcleo para la instalación del cableado, de forma que los múltiples usuarios acceden a la red por medio del punto de acceso. En las ubicaciones que por sus características físicas deban de tener más de un punto de acceso, con el fin de mantener la adecuada cobertura, los puntos de acceso podrán trabajar como maestros o bien como esclavos, estos últimos serían clientes de un punto de acceso maestro.
- **Modo Repetidor:** Este modo se puede usar para extender la señal de forma que el punto de acceso amplifica la señal que recibe para optimizar el rango de acción.
- **Modo Bridge:** Este modo se hace para cubrir grandes distancias, como dos edificios separados. Con dos puntos de acceso conectados entre sí podemos conseguir una red WLAN a distancias considerables.

2.4 Arquitectura WiFi en redes corporativas

Tal y como se ha recalcado anteriormente en una red WiFi existen dos elementos principales [34]:

- Los dispositivos de usuario que actúan como clientes.
- La arquitectura física de acceso y servicios complementarios.

En un ambiente corporativo se supone que los dispositivos que solicitan acceso ya han sido homologados y configurados por el administrador de la red para soportar un proceso de acceso a la red tipo 802.1x utilizando el método EAP-TLS (*Extensible Authentication Protocol–Transport Layer Security*). Por lo tanto, mediante el despliegue inicial los dispositivos han sido previamente configurados y aprovisionados con un certificado de cliente que identifica al usuario y al dispositivo. No obstante, en las redes corporativas puede existir una red de invitados que permita el acceso a la red con limitaciones o incluso que dicha red de invitados sea independiente de la red corporativa y por lo tanto ofrezca servicios independientes de la red corporativa.

En los administradores de la red WiFi recae la responsabilidad de configurar y usar los distintos mecanismos y soluciones disponibles para asegurar que el control a la red se produce de manera segura, basándose en unos pilares básicos:

- Autenticación de usuarios y dispositivos.
- Inventario de equipos y software autorizados.
- Bastionado de los dispositivos autorizados
- Evaluación continua de vulnerabilidades y su remediación.
- Uso controlado de cuentas de administración.
- Limitación de puertos, protocolos y servicios.
- Configuración segura de los dispositivos de red.
- Aplicar las políticas acordes al rol de los usuarios y los dispositivos.
- Verificación continua del comportamiento de los dispositivos.
- Asegurarse de que las comunicaciones se realizan bajo una capa de cifrado.
- Registro de las acciones realizadas con el objeto de realizar futuras auditorías de seguridad.

2.4.1 Topología de las redes WiFi

En una red inalámbrica existe la posibilidad de que sus clientes se comuniquen sin la presencia de un punto de acceso, es la llamada Topología Ad Hoc (figura 2-14), en la cual los dispositivos se comunican entre sí a través de tecnologías como Bluetooth o WI-FI Direct.

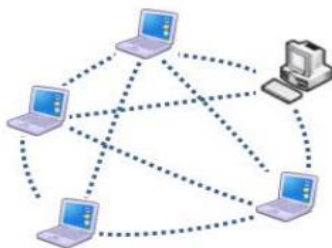


Figura 2-14 Diagrama de una red inalámbrica modo Ad Hoc [34]

Así mismo, existe otra topología de red inalámbrica más compleja y funcional llamada Modo Infraestructura (figura 2-15), en la cual se precisa la presencia de un punto de acceso. Los puntos de acceso pueden ser de dos tipos, punto de acceso inteligente y punto de acceso simple. Los primeros ejecutan de manera independiente las tareas de cifrado y gestión de dispositivos de cliente conectados a ellos. En los puntos de acceso simple, el cifrado y las políticas de seguridad se procesan de forma centralizada en un controlador. En este último, caso, la ventaja es que no se almacenan en cada uno de los puntos de acceso las claves criptográficas.

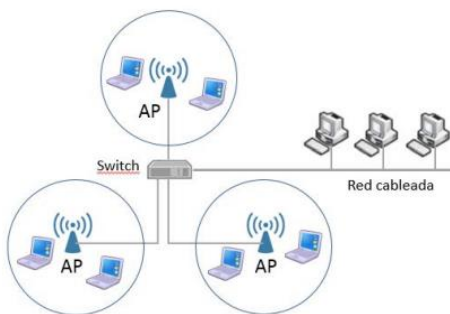


Figura 2-15 Diagrama de una red inalámbrica modo infraestructura [34]

El modo infraestructura es el tipo de red que normalmente se usa en empresas y hogares. En este tipo de infraestructura los clientes acceden a los recursos de la red a través de un punto de acceso o enrutador.

La diferencia entre un punto de acceso y un enrutador inalámbrico, es que el primero está pensado para permitir el acceso inalámbrico a la red cableada, no suele implementar otras funciones típicas de los enrutadores, por ejemplo la función NAT que sí está implementada en los enrutadores.

Existe una última topología que es la topología en malla que resulta de la mezcla de las dos anteriores. En esta topología un equipo actúa como punto de acceso a la vez que crea una red punto a punto, en la cual cualquier equipo puede conectarse e intercambiar tráfico con otro equipo que no esté en el área de cobertura pero si en la malla correspondiente.

2.4.2 Arquitectura de las redes WiFi

A la hora de definir la arquitectura física y lógica de una red WiFi entran en juego una serie de opciones que hacen difícil la generalización de patrones de arquitectura fijos, ya que dichos patrones están influenciados, por una parte, por las necesidades y características propias de la empresa u organización y, por otra parte, se encuentran afectadas por el producto que el fabricante ha elegido como solución de servicio WiFi.

2.4.2.1 Arquitectura Lógica y Física

Respecto a la arquitectura lógica y física de una red corporativa, se pueden definir las siguientes capas funcionales (figura 2-16) [34]:

- **Capa de Datos (Data Plane):** Es la capa encargada de transporta los paquetes de datos en los diferentes sentidos, usuario-red, red-usuario y usuario-usuario.
- **Capa de Control (Control Plane):** Es la capa donde residen los algunos protocolos (no son exclusivos de esta capa), procesos y funciones del servicio WiFi.
- **Capa de Gestión (Management Plane):** Es la capa que permite al administrador la configuración y monitorización del servicio WiFi.

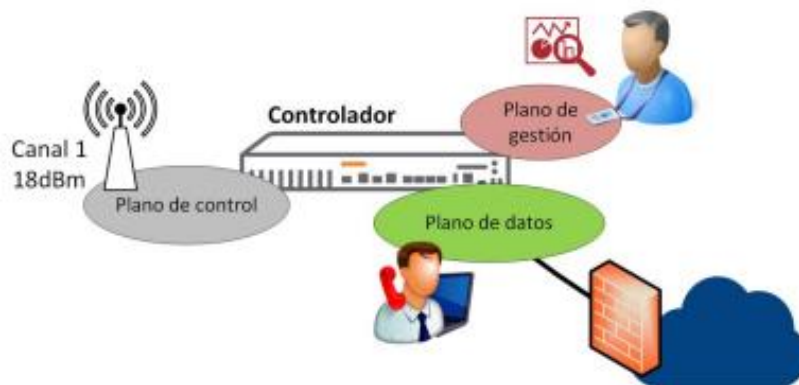


Figura 2-16 Arquitectura lógica de planos funcionales [34]

Como paso previo para la securización de una red WiFi es necesario conocer dónde se ubican cada una de las capas y cómo se relacionan entre sí. Una de las tareas principales del administrador de la red es conocer las diferentes capas con el objeto de configurar correctamente las mismas.

Por ejemplo, podemos encontrarnos con soluciones centralizadas basadas en un controlador (figura 2-17) y una serie de puntos de acceso ligeros dependientes del mismo. La

securización de esta arquitectura sería la dotación de una serie de túneles cifrados mediante IPSec entre los puntos de acceso y el controlador, siendo este último el que gestionaría todas las tareas definidas en las capas de datos, control y gestión.

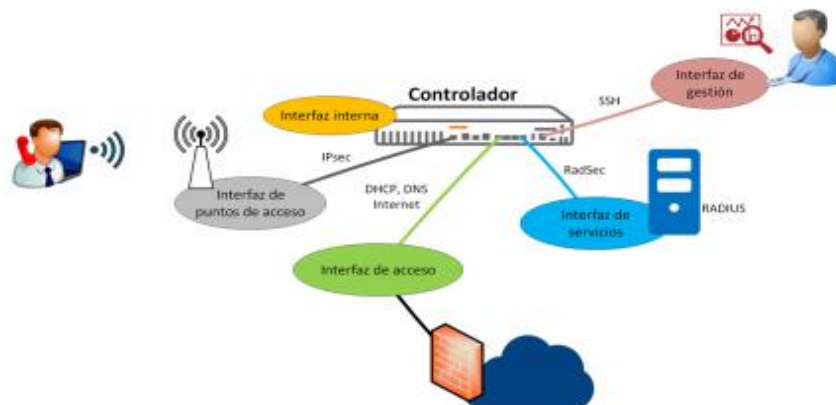


Figura 2-17 Arquitectura de interfaces físicas [34]

El controlador podría actuar como un equipo de nivel 2, con lo que podría realizar la conmutación del tráfico de usuarios hacia la red de acceso o bien podría actuar como un equipo nivel 3 realizando tareas de enrutamiento del tráfico entre diferentes redes de usuario. En la capa de gestión el controlador también asume otras tareas en el plano de control tales como la orquestación en la asignación de canales y potencia. También podría asumir funciones adicionales tales como firewall, filtrado, IDS/IPS, análisis de malware, etc.

En el amplio abanico de posibilidades que nos ofrece la tecnología actualmente, también podemos encontrarnos soluciones descentralizadas sin controlador o “*controller-less*”. En este caso, el plano de datos es cedido a cada punto de acceso y el plano de control puede ser de tipo mallado, en el cual todos los puntos de acceso interactúan como iguales o bien del tipo maestro, en el cual un punto de acceso asume el rol de administrador de dicho plano.

2.4.2.2 Segregación de zonas, redes y roles

La segregación es un método básico en la arquitectura de redes (figura 2-18), que posibilita una mejor defensa de la red y un menor impacto de los incidentes en las mismas. En las redes inalámbricas dicha segregación se consigue a través de un correcto agrupamiento y alistamiento de los distintos equipos que componen la red corporativa. Así mismo, es ideal adoptar la política de confianza cero en toda comunicación que se produzca entre cualquier elemento de la red.

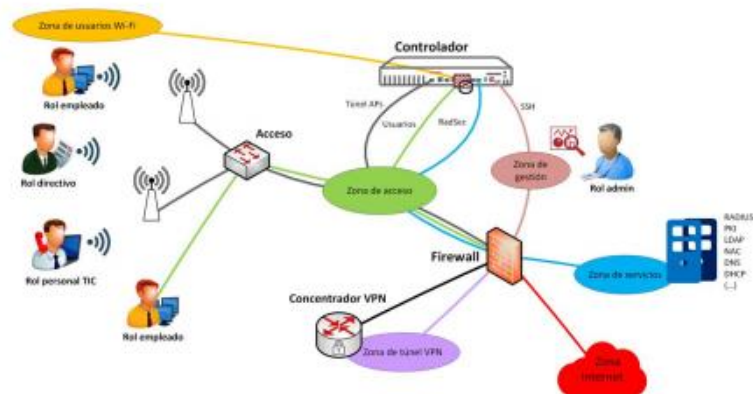


Figura 2-18 Segregación de zonas, redes y roles [34]

Con el objeto de mostrar un ejemplo sencillo, se muestra la creación de zonas, redes virtuales y roles en una arquitectura lógica [34]:

- **Zona de acceso:** Es el conjunto de redes configuradas en los conmutadores de acceso:
 - Red para puntos de acceso: Es una red dedicada a la comunicación entre los puntos de acceso y el controlador, que se establece a través de túneles IPSec.
 - Red de usuarios: Se crean diferentes VLAN en función del departamento, disponibilidad física, nivel de seguridad o rol/perfil de usuario.
 - Red para accesos a servicios: Es una red dedicada al acceso a servicios, por ejemplo, peticiones al servidor RADIUS desde el controlador.
- **Zona de túnel VPN:** El usuario establece un túnel VPN con el concentrador de túneles corporativo, definiéndose una red de confianza protegida de extremo a extremo.
- **Zona de acceso a Internet:** Permite proveer a la red corporativa de acceso a Internet a través de un cortafuego.
- **Zona de gestión:** Realiza las funciones de gestión y administración de todos los sistemas conectados a la misma.
- **Zona de servicios:** Es la zona donde se ubican los servidores corporativos. Debido a la sensibilidad de dicha zona y a la criticidad de la información que dichos servidores pueden alojar, es recomendable hacer una micro-segmentación de la misma y aplicar seguridad extra a cualquier comunicación que se produzca entre los distintos elementos, tanto clientes como servidores.

En el caso de que el controlador actuará como equipo de nivel 3, realizando tareas de enrutamiento, se podrían definir dos zonas en el controlador para los usuarios:

- Zona de redes de usuario WiFi.
- Zona de redes de acceso corporativo.

En redes con controlador, una vez realizada la autenticación del dispositivo, se aplica el concepto de “rol”. El rol afecta al tráfico de usuario, puede suponer o no un cambio de VLAN o una modificación en las reglas de filtrado de red.

De forma genérica, podemos aplicar los siguientes roles [34]:

- Rol de validación: En este estado el usuario ha concluido exitosamente el proceso de autenticación. El cliente permanecerá en este estado mientras se analiza si cumple con los requisitos de seguridad de dispositivo y otros atributos de autorización.
- Rol de cuarentena: Se aplican sobre aquellos usuarios que no cumplan con los requisitos de seguridad.
- Rol de estado saludable: Se aplica sobre aquellos usuarios que sí cumplen con los requisitos de seguridad establecidos. Se permitirá a los clientes establecer un túnel VPN, que asimismo dará acceso a la red.
- Rol de estado saludable con perfil: Este estado surge por la necesidad de crear políticas diferentes en función del perfil de usuario, en cuyo caso se podría crear un rol específico para cada perfil (por ejemplo empleados, directivos, técnicos, etc.).

2.5 Riesgos, amenazas y ataques a redes WiFi

Las redes inalámbricas están bajo la amenaza de la mayoría de los riesgos de las redes cableadas y, además, se añaden los riesgos y amenazas propias de la tecnología WiFi.

Para controlar estos riesgos, aquellas compañías que opten por el uso de tecnologías WiFi deben adoptar salvaguardas que permitan reducir al máximo el riesgo residual así como el impacto de un posible incidente.

Obviamente, como cualquier otra red es imprescindible una continua monitorización del tráfico de red así como el seguimiento de nuevas o antiguas vulnerabilidades que puedan afectar a la empresa.

A continuación se muestran una serie de amenazas que afectan a las redes inalámbricas [35]:

- Debido a una vulnerabilidad desconocida, el equipo podría verse comprometido por tener habilitada la interfaz inalámbrica sin necesidad de contacto físico por parte del atacante.
- A través de la conexión inalámbrica se puede tener acceso a entornos, inalámbricos o no, que estén en contacto con el primero.
- La propagación por espacio libre hace que las comunicaciones puedan ser interceptadas en modo pasivo sin contacto físico con la red y sin posibilidad de detectar dicha captura. También se puede inyectar tráfico malicioso a distancia.
- Se pueden realizar ataques tales como Denegación de Servicio (DoS) a través de inhibidores de frecuencia, paquetes maliciosos, etc.
- En redes sin cifrado o en aquellas en las que se conozca su infraestructura, se pueden desplegar equipos maliciosos, tales como puntos de acceso falsos (*rogue AP*) y realizar la suplantación de los equipos legítimos con el objeto de exfiltrar información y credenciales corporativas.
- Una vez obtenido el acceso a la red, se pueden realizar ataques tipo “*Man in the Middle*” (MITM).
- Se puede obtener acceso a información realizando un análisis forense de un equipo legítimo, previamente sustraído.
- En el caso de que haya redes federadas o conectadas a la nuestra, se puede obtener acceso a través de las mismas, ya que estas podrían tener otras vulnerabilidades susceptibles de ser explotadas.
- Se pueden generar redes falsas en busca de usuarios desprevenidos.
- Se puede obtener información de la entidad propietaria y de los dispositivos de usuario recolectando datos abiertos de fácil captura, por ejemplo: SSID, direcciones MAC, etc.

Las amenazas arriba indicadas tratan de menoscabar los principales activos de seguridad que deben protegerse en toda red [36]:

- Confidencialidad: Característica que consiste en que la información solo debe ser revelada a usuarios autorizados.
- Integridad: Asegura que la información no ha sufrido modificaciones no autorizadas que perturben la veracidad u originalidad de la misma.
- Disponibilidad: La información debe estar a disposición de aquellos usuarios autorizados que deban de tener acceso a la misma cuando se requiera.
- Autenticidad: Propiedad que garantiza la procedencia de la información.
- Trazabilidad: Propiedad que permite determinar la ruta de acceso a la información.

Estas propiedades se verán afectadas por comportamientos inapropiados, maliciosos o descuidados por parte de personal legítimo o atacantes.

Los ataques a redes WiFi pueden ser de carácter pasivo o activo. En el primero de ellos el atacante no interactúa con la red, se limita a escuchar el tráfico de red y a extraer información de la misma. Este ataque suele ser un primer paso previo a la realización de un ataque tipo activo. Debido a su naturaleza pasiva es más difícil de detectar siendo la única manera de contrarrestarlo el cumplimiento de las políticas de seguridad sobre la información y la limitación de la potencia de emisión.

Los principales ataques pasivos son:

- **Sniffing** [37]: El tráfico de la red se expande fuera del área de interés con facilidad, basta con disponer de un equipo con una tarjeta inalámbrica para poder recibirlo. Si el tráfico no ha sido cifrado será accesible para el atacante. También puede ser accesible si se usan protocolos de seguridad no seguros, tales como WEP, TKIP, WPA. Este tipo de ataque es difícil de detectar, por lo tanto, la organización deberá disponer de políticas que limiten la información que circula por la red, el cifrado del tráfico y la limitación de la potencia de emisión.
- **Análisis de tráfico**: El atacante recopila información de la red y analiza dicha información y extrae patrones de tráfico y arquitecturas de la misma. Suele ser un primer paso para futuros ataques más elaborados.

En los ataques activos, el atacante interactúa con la red, recibiendo tráfico de la misma y enviando órdenes a la misma, aprovechando la información adquirida durante el ataque pasivo. El ataque activo supone un mayor riesgo para la organización ya que el atacante está intentando conseguir acceso a nuestros recursos. En una fase más avanzada el atacante ya estaría dentro de nuestra red, buscando afianzarse en la misma y normalmente buscando privilegios elevados en la misma. Dependiendo del grado de defensa y protección de la red puede ser detectado y minimizado.

Los principales ataques activos son:

- **Suplantación** [38]: La principal técnica empleada para la suplantación es la de *MAC Spoofing*. Es una técnica que logra cambiar la dirección MAC del dispositivo de red. Dicha dirección esta codificada en la tarjeta de red por el fabricante y por lo tanto es inalterable. No obstante, a través de las herramientas adecuadas se puede lograr que el Sistema Operativo cree una NIC virtual con una MAC diferente y configurable por el atacante.
- **Punto de Acceso Falso** [39]: Un punto de acceso falso es un punto de acceso inalámbrico que ha sido instalado en una ubicación con la finalidad de atraer a dispositivos móviles susceptibles de atacar. También pueden ser ubicados en un área segura por un empleado o por un atacante sin el permiso explícito del administrador de la red, con el mismo fin.

Suelen encontrarse en aquellas zonas frecuentadas por personas que tienen la intención de conectar sus dispositivos a una red WiFi (restaurantes, bibliotecas, museos, aeropuertos, etc.), con el objetivo de que el dispositivo víctima se conecte al punto de acceso falso y se roben datos confidenciales o la instalación de malware que proporcione un ataque posterior (MITM, spoofing DHCP, secuestro de sesión, etc).

Para que la víctima crea que se trata de un punto de acceso legítimo se suele poner un SSID engañoso (airportMADfreeWiFi, FreeWiFiRestaurante, etc.). Dichos puntos de acceso falsos no tienen seguridad ninguna o es muy débil, no suelen pedir contraseña y su potencia de emisión suele ser alta para captar usuarios desprevenidos. También existe la posibilidad de que una vez el objetivo ha sido cazado por el punto de acceso falso, este le redirija a una página web donde se le solicita rellenar una serie de

campos para continuar con la navegación, incluidos nombre de usuario, contraseñas, datos bancarios, dirección, etc.

- **Modificación [40]:** Una vez el atacante está dentro de la red, puede modificar datos y emitir órdenes. Un método muy extendido es el de “*Man in the Middle*”. El atacante ha conseguido una posición ventajosa colocándose entre el usuario y el proveedor de servicios. De esta manera el atacante adquiere la capacidad de leer, insertar y modificar datos a voluntad.
- **Reactuación:** Consiste en grabar y posteriormente reenviar mensajes legítimos para la realización de operaciones que ya habían previamente realizadas.
- **Denegación de servicio [41]:** El atacante logra que la red quede inhabilitada para ofrecer el servicio para la cual fue creada, por lo tanto, atenta contra la disponibilidad del servicio. Hay varios métodos:
 - Consumo de recursos computacionales, tales como ancho de banda, espacio de disco, tiempo de procesador, etc.
 - Alteración de información de configuración, por ejemplo información de rutas de encaminamiento.
 - Alteración de información de estado, por ejemplo, interrumpiendo conexiones TCP (TCP reset).
 - Interrupción de componentes físicos de la red.

Por lo tanto y según lo anteriormente visto, las características del medio compartido y la accesibilidad de las redes WiFi hacen que un sistema de control de accesos eficaz sea una pieza fundamental en la seguridad de dichas redes. Las principales medidas para asegurar el control de accesos son los siguientes [42]:

- **Filtrado de MAC [43]:** Este método está muy extendido y consiste en la comprobación de la dirección MAC. Su implantación es sencilla, ya que solo es necesario declarar, en el punto de acceso o en un servidor, las direcciones MAC que están autorizadas para conectarse a la red, si bien y tal y como hemos detallado anteriormente, este filtrado puede ser objeto del ataque de suplantación de MAC. Otro problema es que en casos de redes con usuarios no fijos o itinerantes es necesario el proceso de alta y baja constante de los mismos.
- **Portal WEB:** En este sistema de acceso red se precisa un servidor que realice el control de la conexión hacia el exterior. En este método el cliente se conecta sin problemas a la red WiFi, pero no tiene capacidad de conectarse con la web externa ya que es automáticamente remitido a una portal web en el cual debe autenticarse ya sea por usuario/contraseña, tarjeta de crédito, etc... una vez autenticado con éxito el servidor le da acceso a la red. Este sistema está muy extendido y su utilización más común es en espacios públicos a través de los puntos calientes o “hotspots”.
- **Acceso VPN:** Este sistema se basa en la existencia de un servidor VPN que sirve de único punto de conexión con el exterior desde la red. Cuando el usuario se conecta a la WAN, solo se le permite acceso al servidor VPN, lo que le obligará a autenticarse para poder conectarse a Internet. Al estar basado en VPN, se asegura la confidencialidad de las comunicaciones en base al protocolo seguro utilizado por la VPN (IPSec, SSL, TLS...).

2.6 Esquema Nacional de Seguridad (ENS)

Debido al auge que en los últimos años ha supuesto la ciberseguridad y el incremento vertiginoso de ciberataques a nivel mundial, se han creado organismos nacionales e internacionales cuya función es regular y combatir el cibercrimen. En España, entre otros se han creado el INCIBE (*Instituto Nacional de Ciberseguridad*), el MCCE (*Mando Conjunto del Ciberespacio*) y el CCN (*Centro Criptológico Nacional*).

El CCN [44] es el órgano responsable de coordinar la acción de la Administración Pública, para garantizar la seguridad de las tecnologías de la información, así como la de informar sobre la adquisición de material criptográfico de forma coordinada y formar al personal de la Administración especialista en el campo de las tecnologías de la información.

El CCN cuenta con un órgano con capacidad de respuesta a incidentes en el ámbito de la ciberseguridad, el CCN-CERT (*Computer Emergency Response Team*), dicho órgano se encarga de implantar y gestionar medidas preventivas, reactivas y de gestión de seguridad con el objeto de mitigar el riesgo de ataques contra las redes bajo su responsabilidad.

Las redes bajo su responsabilidad son las correspondientes a las Administraciones Públicas (nacional, autonómica y local), así como las correspondientes al sector público, organismos autónomos dependientes de la Administración y aquellas empresas declaradas de interés estratégico para la seguridad nacional y para el conjunto del país.

Por lo tanto, el CCN tiene como misión [44] la de contribuir a la defensa en el ámbito de la ciberseguridad en España, siendo el centro de alerta y respuesta nacional. Así mismo, cooperará y ayudará en la respuesta rápida y eficiente a los ciberataques que se produzcan.

El CCN se rige por el Esquema Nacional de Seguridad que tiene por objeto determinar la política de seguridad en la utilización de medios electrónicos en su ámbito de aplicación y estará constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información.

El Real Decreto 3/2010 [45] de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica, modificado a su vez por el Real Decreto 951/2015 [46], de 23 de diciembre, es de aplicación a las Administraciones Públicas y tiene por objeto asegurar la confidencialidad, integridad, disponibilidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en los medios electrónicos que gestionen en el ejercicio de sus competencias.

Para el cumplimiento de los objetivos previstos en el Esquema Nacional de Seguridad se definen y valoran los fundamentos que van a permitir categorizar sistemas y servicios. Esto supone que dependiendo de la categoría se deberán implementar unas medidas de seguridad u otras, exigiéndose requisitos más restrictivos en función de la información a proteger.

Una red inalámbrica se considera de manera similar a cualquier otro sistema de información. Formado por hardware y software y cuya misión fundamental es dar acceso a recursos, información y servicios de la organización.

Para la determinación de la categoría de la red inalámbrica como sistema de información dentro del Esquema Nacional de Seguridad, hay que tener en cuenta la criticidad de los recursos y servicios de la organización que se establecen y la criticidad de la información que fluye a través de sus conexiones.

La criticidad se establece atendiendo al grado en que se cumple y se protege la información, garantizando, en todo momento, la confidencialidad, disponibilidad, autenticidad, trazabilidad y disponibilidad de la misma.

Así mismo, la valoración del impacto negativo que ocasionará para la organización la pérdida o compromiso de los puntos citados en el párrafo anteriores determinará que la red sea catalogada como BÁSICA, MEDIA o ALTA [47].

Uno de los métodos del Centro Criptológico Nacional para cumplir sus cometidos y adecuarse al Esquema Nacional de Seguridad es la publicación de las Guías CCN-STIC. Esta documentación proporciona un marco de referencia que sirve de apoyo a las Administraciones Públicas para llevar a cabo la tarea de proporcionar seguridad a los sistemas TIC (Tecnologías de la Información y Comunicación) bajo su responsabilidad. Las guías de la Serie 800 son las que regulan aspectos relacionados con el Esquema Nacional de Seguridad.

Para la realización de este trabajo se han tenido en cuenta las guías de la tabla 2-01:

CCN-STIC-001 [36]	Información clasificada en la administración
CCN-STIC-105 [69]	Catalogo de productos TIC
CCN-STIC-201 [93]	Organización y gestión para la seguridad TIC
CCN-STIC-406 [94]	Seguridad en redes inalámbricas basadas en el estándar 802.11
CCN-STIC-801 [63]	ENS Responsabilidad y funciones
CCN-STIC-803 [60]	Valoración de los sistemas
CCN-STIC-804 [47]	Medidas de implantación del ENS
CCN-STIC-816 [59]	Seguridad en redes inalámbricas en el ENS
CCN-CERT_BP_11 [34]	Recomendaciones Redes WiFi

Tabla 2-01 Guías CCN-STIC (elaboración propia)

2.7 Software Libre para Gestión de Redes Inalámbricas

Un aspecto fundamental a la hora de proteger y defender una red WiFi es la monitorización y la gestión de la misma. Existen innumerables soluciones software para realizar dicha gestión y monitorización. De entre todas las soluciones posibles se van a citar algunos ejemplos de software libre que pueden ser de ayuda para controlar el uso que se hace de la red inalámbrica, así como su gestión.

No obstante, el uso de estas soluciones implica una serie de ventajas e inconvenientes que hace necesario un estudio previo sobre la conveniencia de su uso o su descarte. El software libre presenta una serie de ventajas [48]:

- **Accesibilidad:** Es alcanzable para cualquier usuario.
- **Innovación:** Al tener mayor acceso hay un aumento en la capacidad de innovación colaborativa.
- **Menos errores:** El mayor acceso al código del software provoca que hay un mayor número de personas revisando dicho código y encontrando errores en el mismo.
- **Independiente:** Suele ser más ajustable y más proclive a la creación de funciones propias.
- **Bajo costo:** Al tener una comunidad que respalda el desarrollo crea la posibilidad de poder desarrollar productos a bajo costo.
- **Seguridad y privacidad:** Es una característica propia del código abierto. Los usuarios pueden acceder al código en cualquier momento y auditarlo.
- **Crecimiento continuo:** Provocado por el aumento de usuarios y por la renovación de código que los mismos hacen.

Aunque también existen inconvenientes [49]:

- Variedad de versiones: Al ser libre, cualquiera puede crear su propia versión, esto puede fragmentar el mercado y confundir a los usuarios.
- No existe definición de garantía: Prácticamente el software pertenece a la comunidad, por lo tanto, no hay nadie que se haga responsable de dicha garantía.
- Requiere conocimiento técnico: Para revisar y adaptar el código fuente a ciertas necesidades se necesita un conocimiento técnico adecuado.
- El control de calidad: Depende de que la comunidad sea lo suficientemente activa como para revisar el código y mejorarlo. En comunidades poco activas el código no se actualiza y por tanto la calidad se degrada.

Como ejemplos de software libre para la gestión y monitorización de una red inalámbrica podemos citar los siguientes:

- **D.Link** [50]: Permite gestionar hasta 500 puntos de acceso desde una consola software en la web, tanto en local como en remoto. Incluye funciones de optimización de ancho de banda, portal cautivo y gestión integrada de radiofrecuencia.
- **DD-WRT** [51]: Es un firmware alternativo de código abierto basado en Linux adecuado para una variedad de enrutadores WLAN y sistemas integrados (figura 2-19). Como ventaja destaca su fácil instalación, no obstante su configuración puede ser complicada. No obstante, cuenta con gran cantidad de funcionalidades y con una comunidad muy activa.



Figura 2-19 Interfaz usuario DD-WRT [51]

- **Advanced Tomato** [52]: Tomato es un firmware de código abierto para enrutadores basados en *Broadcom*. La interfaz gráfica de usuario (GUI) fácil de usar y un monitor de uso de ancho de banda, calidad de servicio (QoS) más avanzada y restricciones de acceso, nuevas características inalámbricas y modos de cliente inalámbrico, un límite máximo de conexiones P2P más alto, la capacidad de ejecutar scripts personalizados y acceso a través de Telnet/SSH.
- **OpenWrt** [53]: Originalmente basado en línea de comandos con lo que se precisaba un nivel de conocimientos mayor. No obstante, se han creado diferentes interfaces gráficas que han mejorado su manejo. OpenWrt es muy personalizable y se puede añadir funciones adicionales integradas en el software.

- **InSSIDer** [54]: Software de monitorización y exploración de redes inalámbricas (figura 2-20). Tiene un interfaz gráfico fácil de usar y un menú desplegable con múltiples opciones. Muy adecuada para pequeñas redes WiFi tipo doméstico.

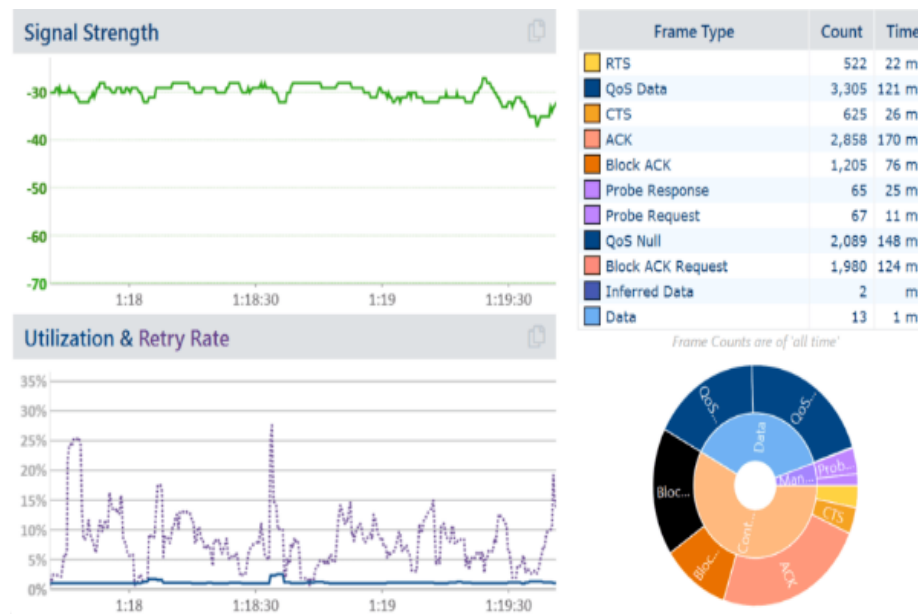


Figura 2-20 Interfaz usuario InSSIDer [54]

- **SolarWinds WiFi monitor** [55]: Esta herramienta permitirá configurar alertas, monitorear la infraestructura y crear informes basándose en diferentes parámetros (direcciones IP, tipo de dispositivo, SSID, canales utilizados, etc.).
- **NetSpot** [56]: Originalmente creada para MAC actualmente está disponible en Windows (figura 2-21). Recopila datos operativos de los puntos de acceso, incluido el cifrado de la red. El detalle que más llama la atención de esta herramienta es el mapa de calor del que dispone. Otras funciones son la capacidad de evaluar la interferencia de la WLAN y el potente motor para realizar informes de forma ágil y rápida.



Figura 2-21 Interfaz usuario NetSpot [56]

En contraposición a lo anteriormente expuesto se citan las herramientas especializadas en la detección de los ataques sobre las redes WiFi [57]:

- **Detectores de puntos de acceso:** Estas herramientas se encargan de observar el tráfico correspondiente a las redes WiFi dentro de su alcance y generar cierto tráfico, al cual los puntos de acceso a su alcance responden, y por lo tanto, se hacen visibles. También permiten conocer los identificadores de conjunto de servicios (SSID) de las redes WiFi de su entorno, aunque no estén en modo promiscuo. Se suele usar para rastrear puntos de acceso sin proteger o abiertos dentro de una ubicación o recorrido. Este tipo de ataque se “wardriving”:

NetSpot	Mac	Interferencias
NetStumber	WS	Scanner
WiFi Scanner	Mac	Scanner
iwScanner	Linux	Scanner
InSSIDer	Windows/Mac/Android	Scanner
KisMAC	Mac	Sniffer/Scanner
NetStumbler	Windows	Wardriving
Xirrus Wi-Fi Inspector	Windows/Linux/Mac	Detector PA falsos

Tabla 2-02 Scanners (elaboración propia)

- **Sniffers:** Estas herramientas capturan el tráfico de las redes WiFi del entorno y lo almacenan en ficheros para su posterior procesamiento. Permiten capturar conversaciones, protocolos, claves, etc:

iStumbler	Mac	Sniffer
SSIDsniff	Linux	Sniffer
Vistumbler	Windows/Linux/Mac	Sniffer
Netsniff	Linux	Sniffer
Kismet	Windows/Linux/Mac	Sniffer

Tabla 2-03 Sniffers (elaboración propia)

- **Crackers:** Se utilizan para romper el tráfico cifrado en una red WiFi. Se alimentan del tráfico que ellos directamente escuchan o por el tráfico proporcionado por un “sniffers”. Para romper la encriptación usan vulnerabilidades conocidas sobre las claves de encriptación (WEP, TKIP, WPA, etc). También hay opciones de búsqueda de claves a través de fuerza bruta.

AirCrack-ng	Windows/Linux	Crackeo red
WPACracker	Windows/Linux	Crackeo red
WepCrack	Windows/Linux	Crackeo red
WepLab	Windows/Linux	Crackeo red

Tabla 2-04 Crackers (elaboración propia)

3 DESARROLLO DEL TFM

En este apartado se desarrollará el proceso de instalación y configuración de una red WiFi basado en el despliegue de tres puntos de acceso sobre un área correspondiente a un edificio de oficinas de tamaño medio, siguiendo las directrices marcadas por el Esquema Nacional de Seguridad (ENS). En la solución propuesta se adoptarán las medidas de seguridad pertinentes dependiendo del nivel de seguridad necesario.

3.1 Descripción del proyecto

El Vicerrectorado de Planificación Académica de la Universidad de Extremadura, tiene unas competencias legales especificadas en la Resolución de 21 de marzo de 2019, BOE nº 62, 29/marzo/2019 [58].

Dicho Vicerrectorado ha decidido instalar un sistema de conexión inalámbrica para facilitar el trabajo entre sus trabajadores. Dicho servicio WiFi también estará disponible para los ciudadanos dentro de sus instalaciones con las limitaciones pertinentes.

El edificio al cual se ha de dotar de WiFi (figura 3-1) está compuesto por una sala diáfana con zonas públicas que se destinarán a zona de espera de los estudiantes y visitas, una zona compuesta por distintas mesas separadas por mamparos destinada al trabajo de los funcionarios, oficinas de jefes de negociado, sala de reuniones, oficina interventor, zona de descanso, aseos y archivo.

La estructura interna está de la oficina se ampliará en detalle posteriormente al desarrollar el modelo de radiación interna.

3.2 Propósito de la red inalámbrica

El propósito es dotar de un punto de acceso a la red de calidad a usuarios, empleados y visitas de la oficina. Dicha red inalámbrica completará a la red cableada existente en la instalación. Así mismo, la red inalámbrica se conectará con la red cableada con el objeto de disponer de conexión con el resto de redes de la Universidad y con Internet.

Como objetivo secundario se facilitará la conexión del personal visitante a una red de invitados.

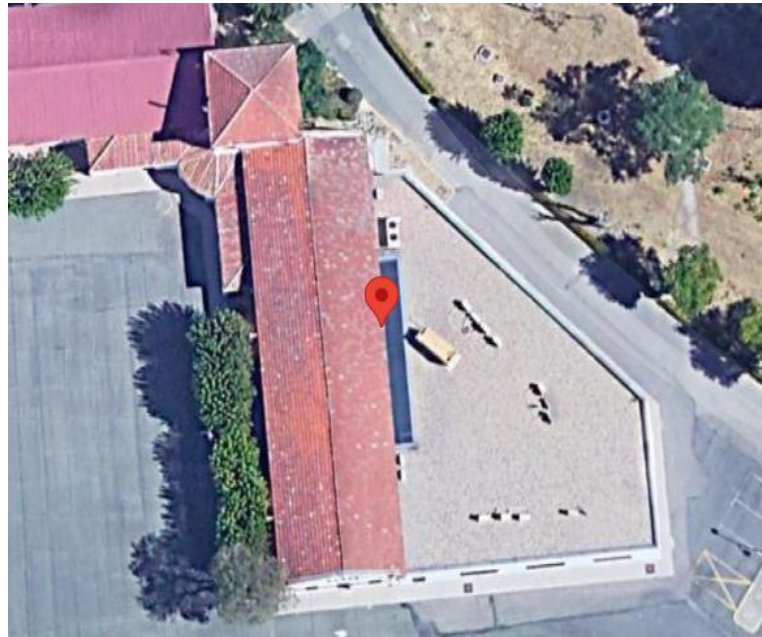


Figura 3-1 Vista aérea de la ubicación de la instalación [73]

La estructura interna de la oficina se ampliará en detalle posteriormente al desarrollar el modelo de radiación interna.

3.3 Uso adecuado de la red inalámbrica corporativa

La red inalámbrica propuesta se considerará como una red de trabajo, por lo que cada usuario será responsable del uso que se haga de la misma.

La organización debe elaborar una serie de Políticas de Seguridad que definan aspectos de seguridad relativos al uso de la misma, tales como quien tiene acceso físico a los equipos de red, quien tiene acceso a la administración de la red, que procedimientos se deben llevar a cabo en el caso de que se detecte un incidente en la red. Obviamente, estas políticas, desarrolladas a través de los procedimientos necesarios, deberán ser objeto de revisiones periódicas.

La red también incluye el acceso a recursos tales como Internet, portal de la Universidad de Extremadura, acceso al entorno académico, investigación, gestión y docencia.

En caso de incumplimiento de las directrices de uso aceptable de la red se podría llegar al caso de bloquear al usuario infractor sin perjuicio de medidas legales a determinar por el Departamento Jurídico de la Universidad.

Para acceder a la red cada usuario dispondrá de un sistema de autenticación basado en nombre de usuario y contraseña. El rol de dicho usuario determinará el número de equipos desde donde puede acceder al sistema, dirección MAC de los mismos, periodos de actividad y registro de actividad del usuario.

Los dispositivos clientes deberán disponer de soporte en el protocolo IEEE 802.1x/EAP para poder acceder a la red en condiciones de seguridad óptimas. Por lo tanto, dichos equipos deben previamente estar normalizados y configurados adecuadamente para su uso dentro de la red.

Previamente a la concesión de usuario y contraseña, el cliente deberá firmar una cláusula de confidencialidad respecto a la información a la que tendrá acceso con ocasión de su acceso a la red. Se le informará de la política interna respecto al uso inadecuado y fraudulento de los medios corporativos puestos a su disposición. La red estará monitorizada en todo momento y se archivarán los registros de actividad para futuras investigaciones.

3.4 Determinación del nivel de seguridad de la red corporativa

Para la configuración de la red se tendrá en cuenta que se trata de una red de uso en una dependencia de la administración universitaria y por lo tanto la configuración se realizará en base al Anexo I de la guía CCN-STIC-803 “*Valoración de los Sistemas en el ENS*” [61], adoptando las medidas establecidas para una red de categoría MEDIA, en base a la criticidad de los recursos e información y de los servicios de la organización que se establecen a través de dicha red, tales como [60]:

- “Que el control de zonas de acceso público se limite a los campus universitarios, puede resultar igualmente un factor a considerar para la categorización de estos sistemas, siempre que no se utilicen mecanismos automatizados de reconocimiento de imágenes”.
- “Los datos de infraestructuras propias (laboratorios, centros de instrumentación científica, etc.) o vinculados a investigación o resultados de investigación no es necesario que gocen de especial protección salvo que puedan suponer un riesgo para la seguridad nacional y la defensa”.
- “Algunos sistemas de las universidades pueden requerir especial protección para garantizar su disponibilidad, puesto que pueden afectar de manera significativa a la normal operativa de la docencia, la gestión o la investigación”.

Obviamente, la criticidad se basa en la medición de una serie de criterios, aplicables a cada una de las propiedades de seguridad, tales como integridad, confidencialidad, disponibilidad, autenticidad y trazabilidad.

Por lo tanto, y en base a los criterios de valoración que marca la Guía CCN-TIC-803 “*Valoración de Sistemas en el ENS*”, concretamente el Anexo I de la misma que se circunscribe al ámbito universitario [61] y, teniendo en cuenta el catálogo de servicios de la oficina y de su función como Subsistema de Gestión Académica, se pueden establecer los siguientes niveles de seguridad (figura 3-2).

SISTEMA “UNIVERSIDAD E.N.S.”					
Denominación del Subsistema	C	I	D	A	T
Gestión Académica	M	M	M	M	M
Apoyo a la Docencia	M		M	M	B
Valor máximo del nivel registrado en las dimensiones de seguridad	M	M	M	M	M
CATEGORÍA MEDIA [C=M, I=M, D=M, A=M, T=B]					

Figura 3-2 Categorización del Sistema “Universidad ENS” [61]

Por lo tanto, y vistos los valores establecidos en la figura 3-2 la categorización de la oficina se establece en un nivel MEDIO, lo que da lugar a una serie de medidas que se deben implementar para alcanzar dicho nivel.

Una de las primeras medidas a instaurar, según la Guía CCN-STIC-816 “*Seguridad en Redes Inalámbricas*” [59] es la de dotar a la red de una serie de medidas organizativas en función del nivel de seguridad establecido. Estas medidas organizativas deberán incluirse en la Normativa, Procedimientos y Procesos de organización.

En cualquier caso, previamente al inicio del despliegue se realizará un análisis y gestión de riesgos que incluya la capacidad del mismo para cumplir los requisitos de confidencialidad,

disponibilidad, integridad y trazabilidad de los datos y acciones que se produzcan en la red. En caso de que dicho análisis de riesgos sobre la red inalámbrica suponga un riesgo evidente contra la seguridad de la información se tendría que valorar la instalación de una red cableada que a priori tendría menos exposición ante amenazas.

3.5 Requerimientos de seguridad de la red inalámbrica universitaria

Los requerimientos de seguridad están basados en la Guía CCN-STIC-816 “*Seguridad de Redes Inalámbricas*” en el Esquema Nacional de Seguridad [59]. La Guía CCN-STIC-816 “*Seguridad de Redes Inalámbricas*”, establece los niveles de seguridad alto, medio y bajo. Debido a las características propias de la oficina de estudio, la información que almacena, la categoría de seguridad más idónea es la de nivel MEDIO.

Por lo tanto, se van a plantear en los siguientes puntos las medidas de seguridad mínimas para que la instalación tenga asegurada dicho nivel de seguridad.

3.5.1 Requerimientos técnicos

Los requerimientos técnicos de seguridad necesarios para el nivel de seguridad requerido son los siguientes [59]:

1.- Normativa de seguridad:

- Uso aceptable de la red inalámbrica.
- Requisitos de seguridad de la infraestructura inalámbrica.
- Requisitos de seguridad de los dispositivos cliente.
- Evaluaciones de seguridad periódicas.

2.- Procedimientos de seguridad y proceso de autorización:

- Autorización de usuarios y dispositivos.
- Operación y mantenimiento.
- Gestión de eventos y registros (logs).
- Monitorización de seguridad continua.
- Auditorías de seguridad periódicas:
 - Se realizarán auditorías de seguridad periódicas de la red por parte de un servicio externo a la Oficina.

3.- Configuración de Seguridad:

- Análisis de cobertura y potencia de radiación de los puntos de acceso para seleccionar su ubicación, minimizando la radiación fuera del perímetro controlado.
- Autenticación:
 - Autenticación del Servidor de Autenticación (AS) frente al dispositivo cliente, a través de certificado.
 - Tipo de autenticación 80211X/EAP (WPA2 Enterprise).
 - Mecanismo de autenticación de doble factor.
 - Contraseñas y claves compartidas con un nivel medio de fortaleza. Así mismo, deberán estar sujetas a una política de renovación y gestión de contraseñas con requisitos de nivel medio.
- Dispositivos clientes:
 - Acceso restringido a la red inalámbrica, solo a los recursos estrictamente necesarios.
 - Inhabilitada la conexión automática a la red inalámbrica.
 - Habilitados solamente los protocolos y servicios necesarios.
 - Modo Ad Hoc inhabilitado.

- Habilitado el método EAP definido para autenticación.
- Habilitación de una red de invitados para los usuarios externos.
- Puntos de Acceso:
 - Deshabilitados servicios, funciones y protocolos no necesarios (principio de mínima funcionalidad).
 - Las conexiones para la administración de los puntos de acceso desde la red cableada interna de la organización deberán contar con mecanismos de protección (SSH, TLS o SNMPv3).
 - Modificar o inhabilitar parámetros por defecto.
 - SSID oculto.
 - Filtrado de MAC.
 - Puntos de acceso fuera del alcance físico de los usuarios y protección del botón reset.
- Bastionado y protección adecuada de la configuración del Servidor de Autenticación.
- Registro de actividad de los dispositivos:
 - Registro de eventos.
 - Registro de acciones de usuarios y administradores.
 - Registro de las conexiones abiertas.
 - Registro de conexiones exitosas y fallidas de usuarios y administradores.
 - Monitorización continua de la red inalámbrica.
 - Monitorización de ataques, escaneos y vulnerabilidades a través de Sistemas de detección y prevención de intrusiones (WIDPS/WIPS).

4.- Destrucción y borrado:

- La destrucción y borrado de material informático perteneciente a la red inalámbrica, especialmente los puntos de acceso, se llevará a cabo por personal externo y habilitado al efecto.

3.5.2 Requisitos operacionales

Para establecer en la red inalámbrica los requisitos establecidos en el Esquema Nacional de Seguridad se han tomado las siguientes medidas operacionales de seguridad en la infraestructura de red [47]:

1.- Arquitectura de Red

Lo que busca esta medida de seguridad es tener una visión global e integral de cómo es el sistema, cómo se gestiona y cómo se defiende. Es una medida básicamente documental y descriptiva.

La arquitectura de red es responsabilidad y debe ser elaborada por el responsable del sistema y debe ser aprobada por el responsable de seguridad.

Para acometer este requisito se van a tener en cuenta dos parámetros:

- Cobertura de los puntos de acceso:
 - Limitando dentro de las posibilidades la radiación no deseada fuera del área de interés (figura 3-3).

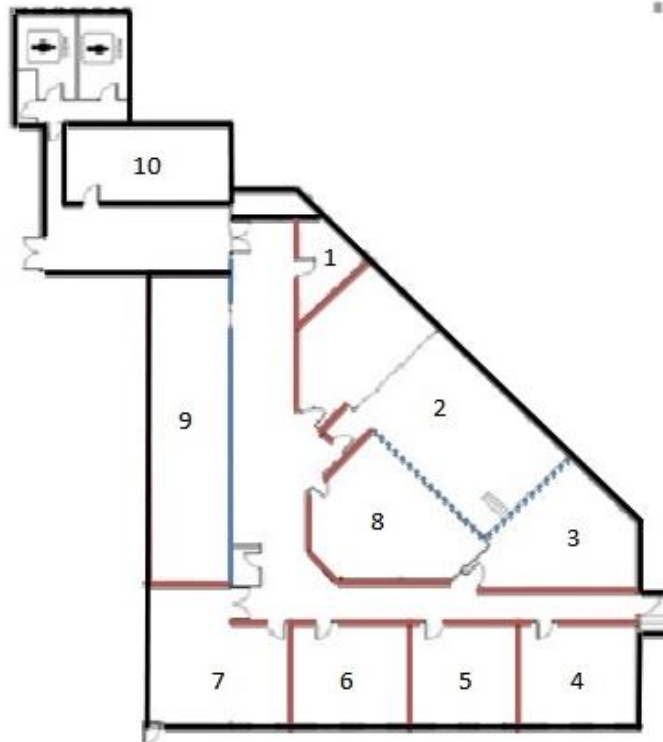


Figura 3-3 Área de interés (elaboración propia)

El área de interés es todo el perímetro en color negro de la figura 3-3. Por lo tanto se evitará la radiación fuera de dicho perímetro (hormigón o ladrillo). El resto de colores en la tabiquería interior representan los diferentes materiales para delimitar espacios interiores, rojo para placas de yeso y azul para vidrio.

Para evitar o minimizar el riesgo de que la señal sea interceptada fuera del área de interés, se estudiará la distribución de puntos de acceso que limiten dicha posibilidad, así mismo se limitará la potencia de emisión de los puntos de acceso. Ambas medidas nos proporcionarán el área de cobertura final de la red.

- La red inalámbrica trabajará en modo infraestructura, este modo de trabajo nos permite un mayor grado de configuración y estandarización de seguridad en el despliegue de los puntos de acceso.

2.- Método de Autenticación o Control de Acceso a la red corporativa

El control de acceso o autenticación cubre un conjunto de actividades preparatorias y ejecutivas para que un determinado usuario o entidad pueda, o no, acceder a un recurso del sistema.

Se asegurará que nadie pueda acceder a ningún recurso del sistema sin previa autorización. En todo caso, deberá quedar registrado en el sistema todo intento fallido o exitoso de acceso al sistema.

Se deberá tener en cuenta que dicho método deberá de guardar un equilibrio entre comodidad de uso y protección de la información, basándose en la criticidad de la información a proteger.

Teniendo en cuenta el nivel de seguridad MEDIO a establecer en la Red, se establecerán los siguientes mecanismos:

- **Identificación:** Se debe asignar un identificador singular a cada entidad (usuario o proceso) que accede al sistema y un rol de cada entidad ante el sistema (administrador, usuario, etc.).
De esta manera, se podrá realizar una trazabilidad de los usuarios que accedan al sistema con las acciones que los mismos realizan dentro del mismo. Así mismo, deberán existir medidas claras y definidas en relación a los usuarios que se dan de baja del sistema, las cuentas inhabilitadas y evitar que un mismo usuario tenga más de una cuenta activa.
- **Segregación de funciones y tareas** [59, 60]: La segregación de funciones tiene como objetivo evitar errores e impedir el uso abusivo basado en privilegios que no corresponden al rol del usuario establecido. Debe existir un documento que especifique qué tareas y funciones son incompatibles en un mismo usuario. Especialmente vulnerables son las tareas y funciones encomendadas al administrador del sistema.
- **Tipo de Autenticación:** El estándar IEEE 802.11i (RSN) permite utilizar dos tipos de autenticación: basada en claves pre-compartidas (PSK) y basada en protocolo 802.1x/EAP. En este caso, nos basaremos en el protocolo 802.1x/EAP que nos proporciona un mayor grado de trazabilidad y nos permite un proceso explícito de autenticación basado en un nombre de usuario y contraseña. Este protocolo es el usado por WPA2 en su versión Enterprise.
- **Mecanismo de Autenticación:** Permite validar la identidad del usuario que pretende acceder al sistema. Los mecanismos de autenticación más comunes recurren a:
 - Algo que se conoce (contraseña).
 - Algo que se tiene (tarjeta, llave, etc.).
 - Algo que se es (característica biométrica).

En el caso de la red de estudio, implantaremos como mecanismo de autenticación el uso de usuario y contraseña.

Existirá una política interna de bastionado de credenciales que será la siguiente:

- Las credenciales deberán activarse una vez estén bajo control efectivo del usuario y serán exclusivamente para dicho usuario. Se forzará al usuario a cambiar de contraseña tras el primer ingreso en la red.
 - Las credenciales caducarán al mes de haberse activado. Pasado 15 días tras la caducidad sin haberse actualizado, la cuenta quedará cerrada para el usuario.
 - Las contraseñas constarán al menos de 10 caracteres en los cuales figurarán, mayúsculas, minúsculas y números.
 - Existirá una memoria de contraseñas por usuario de al menos 5 registros previos con el objeto de que no se repitan contraseñas anteriores.
 - Tras tres intentos fallidos de acceso se procederá al bloqueo de la cuenta, debiendo volver a ser habilitada por el administrador del sistema.
- **Acceso al router** [64]: El acceso local para los administradores de la red, se realizará a través de SSH o HTTPS. Solo el personal con rol de administrador estará autorizado para la administración de los puntos de acceso. Las acciones realizadas por dicho administrador quedarán registradas para posible revisión posterior. Las credenciales de acceso del administrador serán personales e intransferibles, deberán gozar de especial protección y ser identificativas de único responsable.

3.5.3 Requisitos de explotación

Los requisitos relativos a la explotación de seguridad del sistema serán los siguientes [65]:

1.- Inventario de Activos:

El inventario debe cubrir todo el dominio de seguridad del responsable de la seguridad del sistema, incluidos los puntos de interconexión y los servicios que puedan ser prestados por terceros [65, 66].

En el inventario de activos figuran los siguientes datos:

- Identificación del activo: fabricante, número de serie, modelo.
- Configuración del activo: perfil, políticas implantadas.
- Software instalado: fabricantes, productos, versiones, parches aplicados.
- Equipamiento de red: MAC, IP asignada (o rango).
- Ubicación física del activo.
- Persona responsable del activo.

El administrador del sistema contará con un software de gestión de inventario, así como herramientas que le permitan controlar aquellos usuarios que se conectan o desconectan de la red.

2.- Protección de los equipos corporativos

Para la protección de los equipos se seguirán las siguientes normas conocidas por todo el personal usuario del sistema [65]:

- Política de puesto de trabajo despejado: se deberá exigir que los puestos de trabajo permanezcan despejados de todo aquel material que pueda entorpecer el trabajo del personal.
- El material de trabajo que contenga información sensible se guardará convenientemente en cajones o armarios con llave.
- Se debe bloquear la sesión tras constatar 5 minutos de inactividad en el sistema. Para el re acceso al sistema se requerirán las credenciales completas del usuario. Dicho tiempo no podrá ser modificado o anulado por un usuario no administrador.
- Se exigirá que los usuarios cierren sesión y apaguen el equipo al final de la jornada laboral.
- Equipos portátiles corporativos:
 - Existirá un inventario de los equipos portátiles que identifique al equipo y a la persona responsable del mismo.
 - Los equipos portátiles estarán configurados y con las medidas de seguridad mínimas previamente antes de su primer acceso a la red.
 - Se informará por escrito al usuario y, este firmará el correspondiente acuse de recibo, de las medidas implantadas en el equipo, de sus responsabilidades y de las medidas correctivas correspondientes.
 - Los equipos portátiles no podrán contener claves de acceso remoto a la organización.
 - Se informará al usuario de un equipo portátil corporativo de la inconveniencia de usar dicho dispositivo para tareas particulares.
 - En caso de pérdida o robo del equipo corporativo se dará el aviso correspondiente al administrador del sistema y se tomarán las medidas legales necesarias ante las autoridades civiles.

3.- Protección de los puntos de acceso

Para la creación de la infraestructura de la red se instalarán tres puntos de acceso, con el objetivo de dotar de la mayor cobertura posible a la zona de interés. En este caso un punto de acceso actuará como maestro y otros dos como esclavos. La infraestructura se detallará más adelante en esta memoria.

No obstante, los requerimientos de explotación serán los siguientes:

- Se deshabilitará cualquier protocolo de gestión inseguro que pudiese estar habilitado por defecto.
- Se cambiará el SSID por defecto por otro que no aporte información de la organización (definida posteriormente). Así mismo, procederá a su ocultación.
- Basándonos en el principio de mínima funcionalidad, deberán deshabilitarse todos los servicios y funciones de los puntos de acceso que no sean estrictamente necesarios, minimizando la superficie de exposición de la red.
- El puerto de acceso al punto de acceso por defecto deberá ser modificado.
- Filtrado de MAC corporativas:
 - Se creará un listado de direcciones MAC de forma que solo aquellos dispositivos con MAC autorizada podrían acceder a la red. Esta medida no evita ataques a través de “MAC Spoofing”, pero los minimiza.
 - Se deshabilitará las funciones de seguridad WEP, WPA y TKIP.

4.- Servidor de Autenticación

Se dotará de un servidor RADIUS securizado y protegido para el control de acceso a la red.

5.- Registro y trazabilidad de actividades

La monitorización de la red será realizada por personal externo a la misma, no obstante el administrador contará con acceso a SIEM de monitorización a efectos de conocimiento y seguimiento de incidentes. Así mismo, el administrador podrá acceder a un Sistema de Detección de intrusos (IDS), basado en el software Kismet [89].

Se llevará un registro de actividades realizadas por los usuarios con el objeto de detectar posibles riesgos. También se contará con los intentos de acceso fallidos, que si bien pertenecen a personal que aún no accedido a la red, puede permitir la detección de amenazas.

En caso de materializarse una amenaza, el administrador del sistema seguirá las instrucciones que le sean dadas por el centro de seguridad correspondiente y trasladará a los usuarios aquellas recomendaciones que ayuden a minimizar o anular las consecuencias del incidente.

6.- Gestión del Personal

Las medidas implantadas como respuesta a este requerimiento surgen por la necesidad de remediar aquellos problemas causados por el personal con acceso legítimo a la red.

Dichos problemas podrán ser causados de forma deliberada o accidental:

- Se deben definir las responsabilidades por cada puesto de trabajo en materia de seguridad, el trabajador debe conocerlas. El administrador del sistema tendrá constancia escrita (incluida firma del trabajador) de haber comunicado

las responsabilidades al trabajador. También se le informará de las responsabilidades disciplinarias que acarrearán su incumplimiento.

- Se informará por escrito al trabajador, y tendrá que firmar, de su deber de confidencialidad en relación a los datos que maneja con ocasión de sus tareas diarias.
- Dentro de las posibilidades de la oficina se tendrán en cuenta los requisitos de seguridad del puesto de trabajo previamente a la asignación del mismo, incluyendo la verificación de sus antecedentes laborales y disciplinarios.
- Se debe contar con un plan de concienciación y formación para el personal que acceda a la red. Anualmente todo el personal deberá obligatoriamente superar un curso de corta duración (no más de 3 horas). Dicha concienciación de seguridad deberá constar en el expediente del trabajador.

La concienciación refrescará regularmente los siguientes puntos:

- Normativa de seguridad relativa al buen uso del sistema.
- Comportamientos sospechosos.
- Procedimiento de reporte de incidentes de seguridad.

Previamente al acceso de un usuario nuevo al sistema se le deberá impartir la misma formación. El nuevo usuario firmará un documento acreditando que ha recibido la formación necesaria para acceder a la red.

- Para la formación del personal técnico se recurrirá a instancias externas a la oficina, debiendo actualizarse con la regularidad necesaria (nuevos equipos, nuevo software, etc.).
- Existirá una política de baja segura de usuarios del sistema por cese de la actividad en la oficina que asegure la confidencialidad e integridad de la información y el sistema.

3.5.4 Requerimientos de Protección de Datos

Como complemento a los requerimientos de seguridad anteriormente expuestos se añaden otros requisitos establecidos por el Reglamento General de Protección de Datos (RGPD) que también condiciona el uso y los requisitos de la red en los siguientes aspectos [67]:

- Se eliminan las redes WiFi “abiertas”.
- Instalación de un sistema de identificación (*HotSpot*) que proponga aceptar las condiciones de acceso al usuario final. Este software debe permitir la identificación de los usuarios, asociando a su cliente con su nombre, DNI o pasaporte y la identificación de dispositivos a través de la dirección MAC. El usuario deberá aceptar dichas condiciones para poder acceder.
- Se informará al usuario de:
 - La capacidad de recogida, almacenamiento y gestión de datos del sistema.
 - Tipología de datos recogidos.
 - Conexiones con otros sistemas.
 - Prestaciones de servicio.
 - Posibles cesiones de datos afectas.
 - Política de Privacidad con:
 - Finalidad, legitimación y plazos de conservación de los datos.
 - Responsable, encargado y destinatario de los datos.
 - Derechos del usuario, medios para ejercerlos y cualquier información útil para su ejercicio.

3.6 Concepto y definición de la red a desplegar

La red a desplegar se define como una red inalámbrica de uso corporativo para dar servicio a una institución pública. La red inalámbrica será complementaria a una red cableada la cual se integrará en un conmutador (switch) para el acceso a las redes permanentes corporativas.

Este trabajo se centrará exclusivamente en la parte inalámbrica de la red y preferentemente en la parte corporativa (figura 3-4). No obstante, y dado que en el punto 3.3 “Propósito de la red inalámbrica” se citó el uso de parte de los recursos por el personal visitante a la oficina, se darán instrucciones de configuración para que dicha red de visitantes sea efectiva a la par que la red corporativa.

Tal y como se citará y desarrollará posteriormente la red se compondrá de una serie de puntos de acceso los cuales darán cobertura a una estructura permanente dividida en espacios interiores, algunos de los cuales necesitarán más o menos cobertura.

En el caso de la red que se va a desplegar en este trabajo, no se prevé que transporte documentación clasificada. No obstante, sí se considera que trasportará información sensible que exige un mínimo de protección. Motivo por el cual se acometerá un proceso de securización.

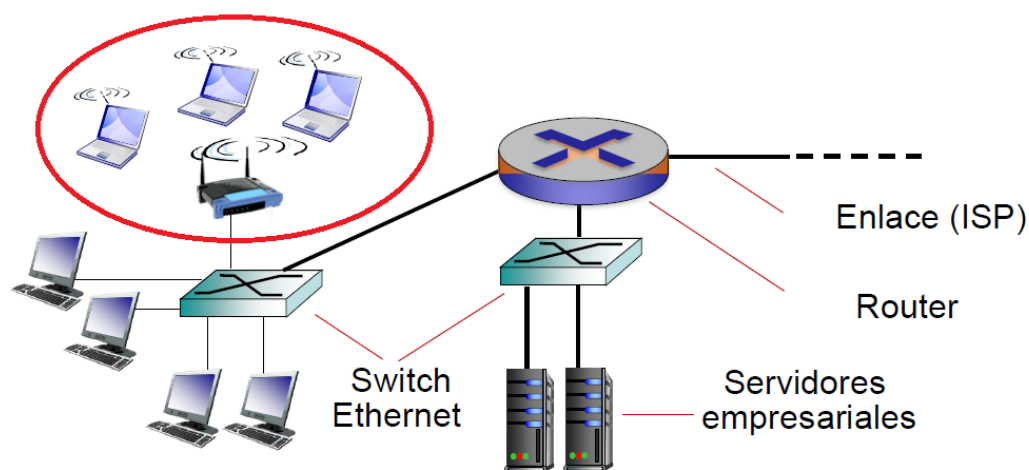


Figura 3-4 Esquema del concepto de la red a desplegar [30]

3.7 Material empleado para el despliegue de la red inalámbrica

Esta parte se centrará en la descripción física del punto de acceso elegido para la implantación de la red así como su configuración inicial. En apartados posteriores se abordará la securización de los puntos de acceso según la normativa anteriormente citada.

Respecto al equipo a adquirir para la materialización de la red, se ha comprobado que soporta los protocolos requeridos y que el fabricante aporta las actualizaciones y soporte necesarios. Se ha aplicado el principio de redundancia con el objeto de que el caso de que un punto de acceso falle (o sea objeto de un ataque) otro pueda asumir su función, aunque supondrá una merma en la cobertura del área de interés. Así mismo, se implantará por parte del administrador de un inventario de equipos de red y clientes como medida básica de seguridad.

3.7.1 Descripción del punto de acceso

Para la implantación de la red WiFi propuesta se ha elegido un router de banda ancha inalámbrico sobre el que se implantarán las medidas obligatorias y recomendadas en la guía CCN-STIC-816 “Seguridad en las redes inalámbricas”.

La guía CCN-STIC-105 “Catálogo de productos STIC” [69] recomienda que el uso de dispositivos de red que proporcionen un mínimo de seguridad. Dicha guía recomienda que la adquisición de productos TIC en aquellas redes que vayan a manejar información nacional clasificada o información sensible debe estar precedida de un proceso de comprobación de que los mecanismos de seguridad implementados en el producto son adecuados para proteger dicha información. Dicha evaluación y certificación del producto es el único medio que permite valorar y acreditar su capacidad para manejar información de manera segura (figura 3-5).

Dentro del catálogo de productos TIC, se ha elegido el producto certificado RUCKUS WIRELESS R610 [70] como punto de acceso de referencia y sobre el que se va configurar el despliegue de la red inalámbrica (figura 3-6).

Las principales características que se han valorado para elegir dicho punto de acceso son las siguientes:

- Soporta los estándares IEEE 802.11 a/b/g/n/ac.
- Producto certificado en Europa.
- Protocolos de seguridad WPA-PSK, WPA-TKIP, WPA2-AES y 802.11i.
- Proporciona una seguridad alta en la valoración respecto al Esquema Nacional de Seguridad. Se recuerda que la valoración de la red se situaba en un valor medio. Por lo tanto, cumple requerimiento.
- Es un punto de acceso recomendado a través de la guía CCN-STIC-105 “Catálogo de productos STIC” y por lo tanto, certificado como hardware de confianza por el CCN.
- Según las especificaciones técnicas y recomendaciones de uso del fabricante el punto de acceso [71] proporciona un rendimiento óptimo en ubicaciones interiores con actividad y densidad media.
- Es configurable vía WEB y SSH.

Ruckus SmartZone WLAN Controllers (SZ-104, SZ-124, SZ 300, vSZ-E , vSZ-H y vSZ-D) & Access Points (R610, R710, R720, T610 y T710)	
Versión	v5.1.1.3
Fabricante	Ruckus Wireless
Familia	Dispositivos de Red Inalámbricos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/03/2021
Revisión de Validez	31/08/2021
Descripción Ruckus SmartZone controllers and Access points es un sistema de acceso WLAN compuesto por múltiples productos operando en conjunto para proporcionar acceso remoto seguro a redes remotas y cableadas. El producto proporciona cifrado punto a punto remoto, gestión centralizada y cumplimiento de políticas AAA (autorización, autenticación y accounting).	

Figura 3-5 Guía CCN-STIC-105 Catálogo de productos TIC [69]



Figura 3-6 Vista exterior punto de acceso Ruckus R610 [71]

Respecto a la cobertura de las antenas (figura 3-6) el punto de acceso elegido proporciona una adaptación dinámica en tiempo real [71] con 512 patrones de radiación con el objeto de establecer la mejor conexión para cada dispositivo. Esto permite conseguir una mejor cobertura WiFi y disminuir la interferencia con otras señales.

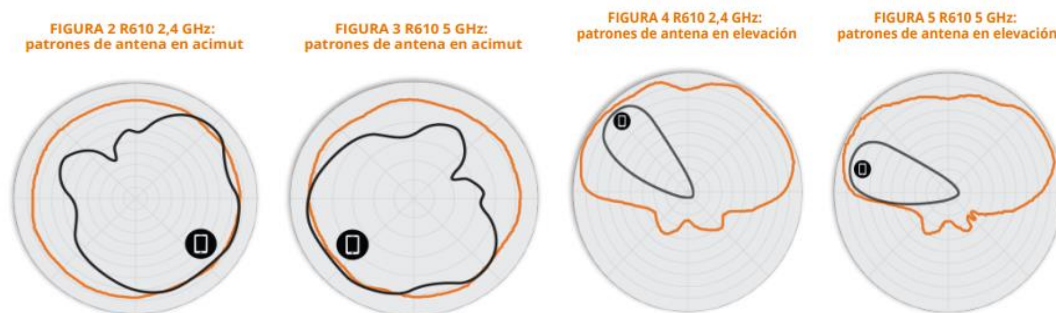


Figura 3-7 Patrones de radiación de la antena Ruckus R610 [71]

Exteriormente el punto de acceso dispone de diferentes puertos de acceso para facilitar la conexión con la red fija [72], así como, testigos para informar del estado del mismo y conectores para la alimentación del punto de acceso.

A continuación se describirán exteriormente las principales características exteriores del punto de acceso:

- Panel delantero (figura 3-8 y 3-9):

- PWR: Detalla si el equipo está alimentado o no. Dependiendo de si parpadea el indicativo o no también nos muestra el estado de operación del mismo:
 - Sin iluminación: El equipo está apagado.
 - Rojo: Equipo en proceso de encendido y carga de la configuración.
 - Verde parpadeante: El sistema está iniciado pero no se ha configurado ninguna dirección IP.
 - Verde fijo: Dirección IP asignada con éxito.
- Indicador 2,4G y 5G: Este indicador señala el grado de ocupación de cada una de las bandas de uso del punto de acceso. También tiene su código de colores:
 - Apagado: Banda está deshabilitada en la configuración del punto de acceso.
 - Amarillo: La banda está habilitada pero no hay clientes conectados.

- Verde: La banda está habilitada y ocupada por clientes.
- CTL/DIR: Indica el estado de conexión a Internet.



Figura 3- 8 Esquema iluminación de los indicadores frontales Ruckus R610 [71]



Figura 3-9 Indicadores frontales Ruckus R610 [71]

- Panel trasero (figura 3-10):

- PoE: Conector RJ45 que incorpora la tecnología PoE (*Power over Ethernet*) que posibilita la alimentación eléctrica al equipo a través del cable que se usa para la conexión a la red.
- Conexión WAN.
- Conector alimentación 12V.
- Puerto USB 2.0 conector tipo A.



Figura 3-10 Indicadores traseros Ruckus R610 [71]

3.7.2 Configuración inicial del punto de acceso

El propio punto de acceso dispone de una configuración estándar disponible en la nube del fabricante de fácil acceso a través de un ordenador. Dicha configuración básica, que se aplicará en un primer momento, permite desplegar un punto de acceso a través de un asistente web. La configuración básica está orientada al despliegue del equipo en entornos no seguros o con seguridad mínima.

Debido a los requerimientos de seguridad, y partiendo de la configuración básica, se implementarán posteriormente medidas adicionales con el objeto de bastionar nuestra red y adaptarla al Anexo I de la guía CCN-STIC-803 “*Esquema Nacional de Seguridad*”, deshabilitándose aquellas configuraciones que puedan suponer una vulnerabilidad para la red.

Para la configuración securizada existe la posibilidad de configurar el punto de acceso a través de un software basado en Linux, por ejemplo OpenWRT, Tomato, DD-WRT a través de la web de configuración vía HTTPS y a través de SSH con asistentes tipo PuTTY.

A continuación se describirá la configuración inicial web del punto de acceso a través de los siguientes hitos:

1.- Configuración por defecto:

Los datos correspondientes a la configuración inicial del punto de acceso figuran en la documentación que se proporciona con el equipo (figura 3-11) y en una etiqueta en la parte no visible exterior del punto de acceso (figura 3-12):

```
ISEC S.A. - RUCKUS NETWORKS

+++++
Dirección IP por defecto =      192.168.0.1
Máscara por defecto =         255.255.255.0
Usuario por defecto =          super
Contraseña por defecto =       sp-admin
+++++
```

Figura 3-11 Configuración por defecto del punto de acceso en la documentación [71]



Figura 3-12 Configuración por defecto del punto de acceso en el exterior del punto de acceso [71]

2.- Verificaremos los detalles de la tarjeta de red del punto de acceso (figura 3-11).

Detalles de la conexión de red:

Propiedad	Valor
Sufijo DNS específico p...	
Descripción	Realtek PCIe GBE Family Controller
Dirección física	50-7B-9D-D4-80-D3
Habilitado para DHCP	No
Dirección IPv4	192.168.0.1
Máscara de subred IPv4	255.255.255.0

Figura 3-13 Detalles de la conexión a red [97]

3.- Lanzamos un PING a la IP del punto de acceso para verificar que hay conexión (figura 3-14).

```

C:\> Seleccionar Símbolo del sistema - ping -t 192.168.0.1
Respuesta desde 192.168.0.1: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.0.1: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.0.1: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.0.1: bytes=32 tiempo=10ms TTL=64
Respuesta desde 192.168.0.1: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.0.1: bytes=32 tiempo=1ms TTL=64

```

Figura 3-14 Verificación ping IP 192.168.0.1 (elaboración propia)

4.- Una vez verificada la conexión habrá que dirigirse al navegador web:

Escribimos la dirección IP de acceso al punto de acceso (192.168.0.1). Posiblemente surgirá un error de seguridad debido a que el navegador no reconoce el certificado SSL del punto de acceso. Se ignora el aviso pulsando “continuar en la página web (no recomendado)” y se continuará con la configuración.

5.- Aparecerá la consola de acceso al gestor del punto de acceso (figura 3-15) y se introducirán las credenciales por defecto proporcionadas por el fabricante (figura 3-16).



Figura 3-15 Consola de acceso web a la configuración del punto de acceso [71]

Si los datos son correctos se abrirá a la consola de configuración (figura 3-16).

Ruckus T610 Multimedia Hotzone Wireless AP

Status

- Device
- Internet
- Local Subnets
- Radio 2.4G
- Radio 5G

Configuration

- Device
- Internet
- Local Subnets
- Radio 2.4G
- Radio 5G
- Ethernet Ports
- Hotspot

Maintenance

- Upgrade
- Reboot / Reset
- Support Info

Administration

- Management
- Diagnostics
- Log

Status :: Device

Device Name: lsec_Piso2_Sala1
 Device Location:
 GPS Coordinates:
 Power Consumption Mode: PoE Injector
 MAC Address: D8:38:FC:19:8B:00
 Serial Number: 511604006011
 Software Version: 104.1.0.0.1013
 Uptime: 18 mins 7 secs
 Current Time (GMT): Fri Jul 14 06:19:45 2017

LAN Port Status [Refresh](#)

Port	Interface	802.1X	Logical Link	Physical Link	Label
0	eth0	None	Up	Up 100Mbps full	10/100/1000 PoE
1	eth1	None	Down	Down	10/100/1000

Figura 3-16 Consola de administración del punto de acceso [97]

En la parte derecha de la consola, en el apartado STATUS, se puede observar los detalles técnicos del dispositivo que vienen configurados de fábrica, incluidos el nombre por defecto, que cambiaremos posteriormente, la dirección MAC, número de serie, etc. Así mismo, el puerto eth0 está abierto por defecto. Dicho puerto se aprovechará posteriormente para la salida de tráfico hacia la red cableada. En la opción “*Ethernet Ports*” se pueden configurar las opciones disponibles para habilitar o deshabilitar los puertos Ethernet.

En la parte izquierda de la consola nos aparecen las diferentes opciones de trabajo:

- Estado: Muestra el estado actual del dispositivo, equipos conectados, etc.
- Configuración: Permite realizar la configuración del punto de acceso.

- Mantenimiento: Permite realizar actualizaciones manuales, reiniciar o resetear el equipo e información sobre el soporte.
- Administración: Permite opciones de gestión, diagnosis y almacenamiento de los registros (logs).

6.- Configuración del dispositivo (*Configuration Device*) (figura 3-17):

- Nombre del dispositivo:
 - Punto de acceso maestro: AP1
 - Puntos de acceso esclavos: AP2 y AP3
- Localización: Por motivos de seguridad se ha completado con una localización ficticia.
 - 55°55'55"N 5°55'55,5"W
- LED Control: Permite la opción de deshabilitar los testigos LED del exterior del AP, excepto el LED de encendido. Dado que los puntos de acceso se colocarán fuera del alcance de los trabajadores, se configurará para que muestre los testigos, como primera medida de supervisión de su funcionamiento.
- Service Provider Login: Se cambia el nombre de usuario y contraseña de acceso al punto de acceso que viene por defecto de fábrica (figura 3-12):
 - Usuario administrador: AdminTFM2021
 - Contraseña: hNFzRM957RS3SuuMRpKx
- TACATS – Estado: [74] Es un protocolo de autenticación remota privativo de Cisco, comúnmente usado en redes Unix, que se usa para comunicarse con un servidor de autenticación. TACATS permite a un servidor de acceso remoto comunicarse con un servidor de autenticación para determinar si el usuario tiene acceso a la red. TACATS está documentado en el RFC 1492 [75]. Se marcará la opción correspondiente a efectos de la futura instalación de un servidor de autenticación RADIUS.

Configuration :: Device

Device Name:

Device Location:

GPS Coordinates: , (e.g. 37.388, -122.0258633)

LED Control: ☐ Disable Status LED(s)

Service Provider Login

Username:

Current Password:

New Password:

Confirm New Password:

Login remote authentication

TACACS+ State: ☐

Figura 3-17 Consola configuración del dispositivo [97]

7.- En este apartado se configura la salida a Internet (figura 3-18), en este caso se configurará el apartado de “*Internet Connection Settings*” con la dirección IP correspondiente a la red cableada. Con esta configuración la red tendrá salida a la red cableada.

Configuration :: Internet

NTP Server:

Management VLAN: (Need to reboot for change to take effect)

IPv4 Connection Type: ☐ DHCP ☒ Static IP ☐ PPPoE

Internet Connection Settings

IPv4 Address:

IPv4 Subnet Mask:

IPv4 Gateway:

IPv4 DNS Mode : ☒ Auto ☐ Manual

IPv6 Connection Type: ☒ Auto Configuration ☐ Static IP

IPv6 Primary DNS Server:

IPv6 Secondary DNS Server:

Figura 3-18 Configuración Internet [97]

8.- Configuración del segmento radio en 2,4G (*Configuration Radio 2,4 G*): Al acceder a dicha opción aparecen las opciones principales del punto de acceso para la configuración del segmento radio del punto de acceso en la banda de 2,4 GHz.

Se va configurar la red en base a la banda 2,4G debido a las siguientes razones:

- En una banda ampliamente compatible con los dispositivos móviles.
- Es menos sensible a muros, separaciones y con mayor alcance.
- En la zona de despliegue la saturación del espectro es baja.

La configuración del segmento radio 2,4 G es la siguiente:

- Common: Aparecen datos por defecto que se adaptarán a cada red (figura 3-19).

Configuration :: Radio 2.4G :: Common

Common | Wireless 1 | Wireless 2 | Wireless 3 | Wireless 4 | Wirel

Radio Network:

Wireless Mode:

Channel:

Channel Width:

Country Code:

Advanced Settings:

[Restore previous settings](#)

Figura 3-19 Configuración “common” [97]

En el apartado correspondiente a “*Channel*” puede dejarse la opción “*SmartSelect*” mediante la cual el punto de acceso busca el canal menos saturado para su uso o seleccionar un canal de trabajo fijo. Se dejará esta opción por ser la que mejor se adapta a la saturación real del área.

- Wireless: (figura 3-20, 3-21 y 3-22) Se van a configurar dos redes inalámbricas, Wireless 1 y Wireless 2 según los parámetros que figuran en la tabla 3-1:

The screenshot shows the 'Wireless 1' configuration tab. Key settings include: Wireless Network: Wireless 1; Wireless Availability: Disabled; Broadcast SSID: Enabled; SSID: Wireless1; Packet Forward: Bridge to WAN; Hotspot Service: None; Access VLAN: 1; Encryption Method: Disabled.

Figura 3-20 Configuración Wireless 1 y Wireless 2 [97]

	Red Corporativa	Red Invitados
Wireless Networks	Wireless 1	Wireless 2
Wireless Availability	Enable	
Broadcast SSID	Disabled	Enable
SSID	TFM2021	UPC-Invitados
Packet Forward	Bridge to WAN	
Hotspot Service	Enable	
Encryption Method	Enable	

Tabla 3-01 Parámetros de configuración redes (elaboración propia)

El apartado Access Control permite realizar una de las funciones básicas de seguridad de cualquier punto acceso, el “Filtrado de MAC”. Esta medida básica de seguridad permite que solo aquellas MAC autorizadas previamente puedan acceder al router:

The screenshot shows the 'Access Control' section with the 'Edit Settings' button highlighted by a red rectangle.

Figura 3-21 Configuración lista de acceso [97]

The screenshot shows the 'Access Control Table' with a table of MAC addresses. The selected radio button is 'Allow only stations listed in the Access Control Table'.

Address	Remove?
64 : DB : 43 : 08 : 48 : 93	Cancel

Figura 3-22 Agregación MAC [97]

En este punto realizaremos el alta de todas las MAC que están autorizadas a acceder a la red. Dicha medida es fácilmente evitable a través de MAC Spoofing, aunque da un primer nivel de seguridad contra los atacantes más inexpertos.

El punto de acceso tiene cuatro modos de funcionamiento de los cuales se usará “Bridge to WAN” (figura 3-23).

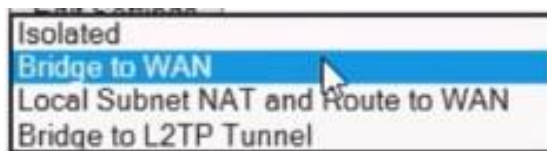


Figura 3-23 Modos de funcionamiento del punto de acceso [97]

Bridge to WAN: El punto de acceso deja pasar todo lo que recibe por el puerto LAN, volviéndolo inalámbrico sin interferir en el tráfico, por lo tanto actúa como un conmutador inalámbrico.

Así mismo, hay que configurar las opciones de encriptado (figura 3-24):



Figura 3-24 Configuración cripto del punto de acceso [97]

- Wireless 1 (red corporativa):
 - Exclusivamente WPA2, 802.1x y AES.
 - Contraseña acceso: j9sxTwrhFyhz3CKYIQN4
- Wireless 2 (red invitados):
 - WPA+WPA2, PSK y AES
 - Contraseña de acceso: UP-Invitados (coincide con el SSID)

9.- Configuración Hotspot (figura 3-25):

Si se desea configurar el punto de acceso para que se comunique previamente con un servidor de autenticación, se ha de recurrir a la opción “Hotspot” en la cual se indicará la dirección primaria y secundaria del servidor RADIUS. Esta opción se habilitará para la red corporativa.

Para la red de invitados la opción elegida será redirigir la autenticación a un “Hotspot” en el cual se tendrá que autenticar el usuario mediante contraseña y donde se le comunicará los datos relativos a protección de datos, que el usuario tendrá que validar para acceder a la red de invitados.

Figura 3-25 Configuración Hotspot [97]

- 10.- En este último paso vamos a indicar al punto de acceso que no va a ser controlado (figura 3-26) a través de una controladora. En caso contrario se habilitaría la opción “*Set controller address*” donde habrá que indicarle la dirección IP del controlador. También en esta pantalla se deshabilitan las opciones de gestión a través de Telnet y HTTP Access, dejando únicamente las opciones de acceso al punto de acceso a través de HTTPS Access y SSH. De la misma manera cambiaremos el puerto de acceso SSH del 22 (preconfigurado) por el puerto 1024.

Figura 3-26 Configuración controlador y acceso al punto de acceso [97]

Una vez acabada la configuración se pulsará “*Update Settings*” saldrá un aviso de que los parámetros han sido guardados y disponiendo en ese momento de dos redes radiando en 2,4 Ghz.

En esta primera etapa los clientes deberían estar recibiendo señal de ambas redes con sus correspondientes SSID. En un siguiente paso se procederá a ocultar el SSID de la red corporativa.

3.7.3 Otro material necesario

Como soporte y parte de la implantación de la red se cuenta con un ordenador permanentemente funcionando que aportará las funciones:

- Gestión integral de la red.
- Puesto de trabajo del administrador.
- Acceso web a los distintos puntos de acceso.
- Consola servidor RADIUS.
- Base de datos MySQL.
- Acceso al SIEM del centro de operaciones de seguridad.
- Consola KISMET.

El ordenador de gestión estará ubicado en la Sala 4 y contará con las medidas de seguridad física necesarias para evitar la entrada no autorizada al mismo.

3.8 Despliegue de la Red

3.8.1 Estudio de la cobertura de la red

Para el estudio de la cobertura de la red propuesta se va a realizar un mapa de calor especificando las características físicas del área de interés. Con dicho estudio se pretende decidir el número, localización y potencia de transmisión de los puntos de acceso.

El edificio en el cual se desplegará la red WiFi planteada es el que se muestra en la figura 3-27. Las características físicas del mismo son las siguientes:

- Superficie total: 360 m².
- Muros exteriores (color negro) de hormigón de 15 cm de espesor.
- Muros interiores:
 - Color azul continuo: Cristal tintado de 10 mm de espesor.
 - Color azul discontinuo: Cristal sin tintar de 10 mm de espesor.
 - Color rojo: Doble placa de cartón yeso (tipo pladur) estándar de 13 mm de espesor, con aislante térmico y acústico entre ambas placas.
 - Las puertas exteriores son de doble plancha metálica, con apertura antipático.
 - Las puertas interiores son de madera maciza.
 - Las ventanas exteriores son de doble cristal tintado y disponen de rejas de seguridad.
 - El edificio se encuentra en un entorno relativamente aislado, no siendo habitual la concentración de tráfico, personas o medios electrónicos.

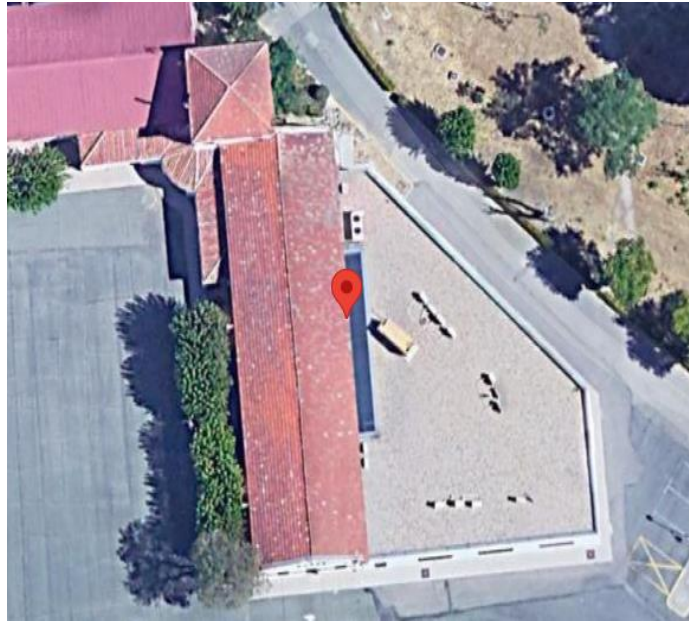


Figura 3-27 Vista aérea del edificio propuesto de despliegue [73]

Respecto a la cobertura interna del edificio se muestra en la figura 3-28. El edificio está dividido en las siguientes partes:

- Sala 1: Sala de descanso de personal.
- Salas 2, 3 y 8: Sala principal de trabajo de los trabajadores.
- Salas 4: Oficina del Jefe de Seguridad y administrador de la red.
- Sala 5 y 6: Oficina del Jefe de Departamento e Interventor.
- Sala 7: Sala de reuniones.
- Sala 9: Sala de espera para personal visitante.
- Sala 10: Almacén.



Figura 3-28 Distribución interna del edificio (elaboración propia)

No todas las salas arriba indicadas (figura 3-29) no todas necesitan cobertura WiFi, la prioridad en su cobertura es la siguiente:

- Cobertura prioritaria: Salas 2, 3, 4, 5, 6, 7 y 8.
- Cobertura deseable: Sala 9.
- Cobertura no deseable: Salas 1 y 10.

Teniendo en cuenta la estructura interna y externa del edificio y la prioridad en la cobertura del señal WiFi, se procede a realizar un estudio mediante un software especializado en dicha materia para analizar el número y distribución espacial de los puntos de acceso necesarios y en su caso la potencia de transmisión necesaria.

Respecto a la potencia de transmisión se reducirá lo necesario para evitar, en la medida de lo posible, su cobertura fuera del edificio.

El software elegido para dichos análisis es la suite “Acrylic” en sus distintas modalidades. Primeramente, se empleará el software “Acrylic Heatmaps WiFi” [77] (figura 3-29) para realizar un estudio de cobertura WiFi, y detectar interferencias y validar el despliegue. También permite predecir la propagación de la señal WiFi y obtener los datos necesarios para ubicación y configuración óptima de los puntos de acceso.



Figura 3-29 AcrylicHeatmaps WiFi [76]

Como resultado del estudio con “Acrylic Heatmaps WiFi” se detecta que la cobertura óptima la proporcionan tres puntos de acceso en la banda de 2,4 GHz distribuidos según la figura 3-30. Bajo este despliegue se da cobertura al área de cobertura prioritaria y al área de cobertura deseable. Así mismo, la estructura exterior del edificio basado en muros de hormigón atenúa la señal, aunque no llega a anularla.



Figura 3-30 Colocación de los Puntos de Acceso [76]

En la figura 3-30 las zonas de color azul son áreas de cobertura de menor calidad. En dichas zonas el nivel de señal se sitúa en 62 dBm y 50 mW, por lo tanto, se consideran aptas para una conexión WiFi [77]. Con el objeto de reducir la señal en el exterior del edificio se procede a reducir la potencia de emisión de los puntos de acceso:

- PA1: 15 dBm / 32 mW (Maestro)
- PA2: 15 dBm / 32 mW (Esclavo 1)
- PA3: 15 dBm / 32 mW (Esclavo 2)

Tras este ajuste de potencia de transmisión y nivel de señal, el mapa de calor es el que se muestra en la figura 3-31. Se destaca que en el interior del edificio la cobertura permanece en valores óptimos y se reduce sensiblemente la señal radiada fuera del edificio. Esta reducción de emisiones exteriores es una medida de seguridad básica y deseable en toda red WiFi.

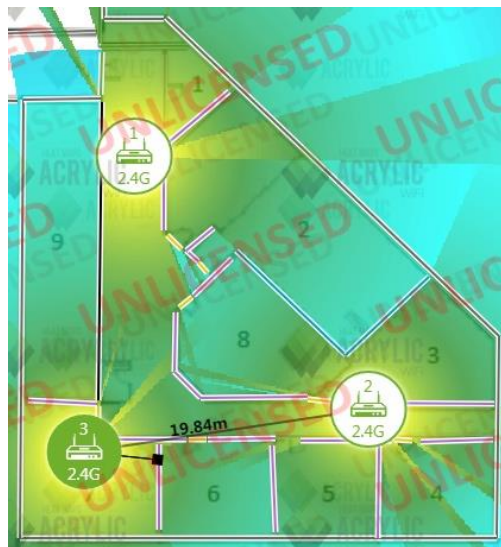


Figura 3-31 Reducción de la potencia de emisión [76]

Se realiza un estudio, en modo pasivo, de las redes WiFi radiantes en la zona a través de la herramienta “Acrylic Wi-Fi Home”, con el objeto de detectar posibles redes vecinas que puedan perjudicar la calidad de la cobertura de nuestra red. Se detectan las mostradas en la figura 3-32:

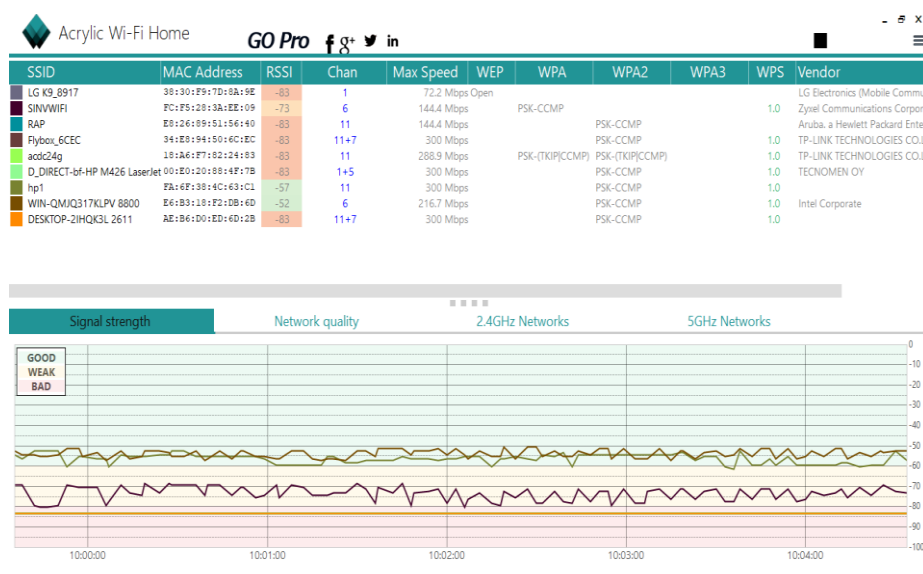


Figura 3-32 Redes WiFi radiantes en la zona de interés [77]

Respecto a los canales, visto el nivel de saturación de los mismos figura 3-33, se adopta el criterio de configurar los puntos de acceso para que se adapten de forma automática a aquellos canales con menos saturación.

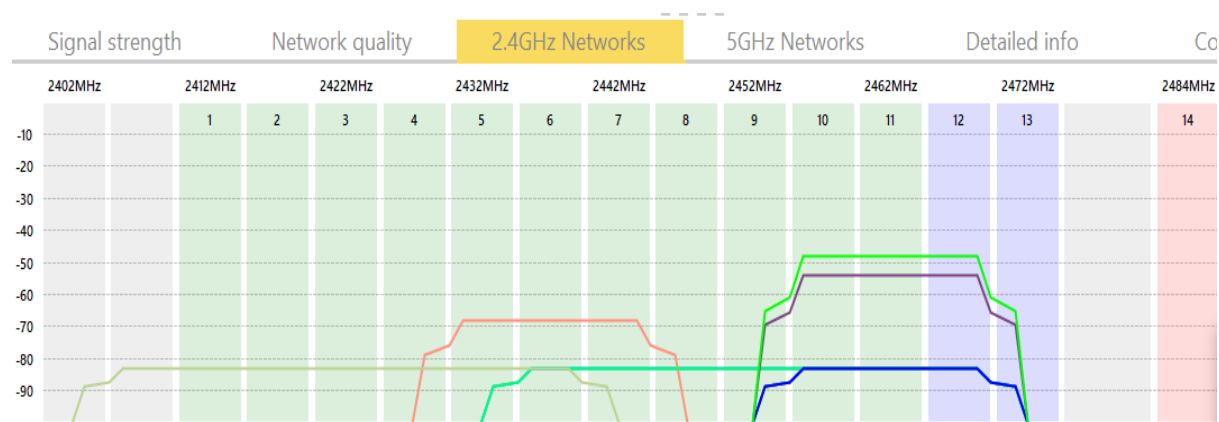


Figura 3-33 Saturación de canales en la banda de 2,4 Ghz [77]

Existen otros dispositivos comunes que pueden generar interferencias o ruido en la infraestructura de nuestra red [78] tales como, microondas, cámaras de CCTV inalámbricas, dispositivo Bluetooth y Zigbee, teléfonos inalámbricos, inhibidores, etc.

Para evitar las interferencias procedentes de dichos dispositivos se toman las medidas siguientes:

- Microondas: No existe dicho dispositivo en la zona de interés.
- Cámaras CCTV inalámbricas: El sistema de CCTV es cableado.
- Dispositivos Bluetooth o Zigbee: En principio no existen dispositivos de este tipo corporativos en la zona de interés. Podrían existir dispositivos de carácter personal, aunque se considera que no afectan significativamente a la calidad de la señal debido a su poca potencia de emisión.
- Teléfonos inalámbricos: Se ha procedido a sustituir los teléfonos inalámbricos problemáticos por otros que trabajen en un ancho de banda distinto o en su caso por teléfonos cableados.
- Inhibidores: No existen inhibidores en la zona de interés.

Por lo tanto, y debido a los pocos elementos sospechosos de aportar ruido a la red, a priori, se omite la realización de un estudio más exhaustivo del ruido ambiental.

3.8.2 Valoración de opciones de despliegue

Teniendo en cuenta el despliegue de los puntos de acceso, la cobertura y potencia de los mismos, los valores mostrados respecto a la saturación del área de estudio y la posible presencia de elementos externos que pudieran generar interferencias se estima que el área es apta para la instalación de una red inalámbrica en la banda de 2,4 GHz, con una potencia media de 15 dBm/32 mW y preferiblemente en canales bajos.

El despliegue de la red WiFi se puede plantear, al menos, bajo tres puntos de vista diferentes:

- **WDS** (*Wireless Distribution System*) [79]: Es una forma de conectar diferentes dispositivos WiFi (rúters o puntos de acceso), de forma inalámbrica y con el objetivo de

ampliar la cobertura de radiación de un mismo SSID (figura 3-34). También nos permite conectar dos dispositivos para interconectar diferentes subredes.



Figura 3-34 WDS (Wireless Distribution System) [79]

Esta opción tiene ventajas e inconvenientes que conviene evaluar antes de su aplicación:

- **Ventajas:**
 - La principal ventaja es que se mantiene la dirección MAC original de los paquetes.
 - Se amplía la cobertura WiFi de una manera relativamente fácil.
 - Mantiene el mismo SSID y contraseña en toda el área de cobertura.
- **Inconvenientes:**
 - Los equipos deben de ser compatibles.
 - El rendimiento de la red se reduce a la mitad con cada salto.
- **Red mallada (Mesh) [80]:** Este sistema se compone de un punto de acceso central o maestro y uno o varios puntos de acceso satélites o esclavos (figura 3-35). El punto de acceso maestro será el que se conectará a la red exterior cableada y los puntos accesos esclavos ampliarán el radio de cobertura de la red. La comunicación se produce entre los puntos de acceso esclavos y el punto de acceso maestro, así como entre los puntos de acceso esclavos entre sí.

Este procedimiento también tiene ventajas e inconvenientes a valorar:

- **Ventajas:**
 - Se mantiene el mismo SSID y contraseña en toda el área de cobertura.
 - La red puede autogestionar el tráfico de datos para ofrecer la ruta más corta y eficiente al tráfico de red.
 - Calcula de manera transparente para el cliente a qué punto de acceso debe conectarse en cada momento, valorando la potencia y la calidad de la señal.
- **Inconvenientes:**
 - La colocación de los puntos de acceso debe ser la ideal, en caso contrario podría ser contraproducente para el rendimiento de la red.
 - No solucionan problemas de cobertura ocasionados como consecuencia de problemas estructurales del área a cubrir.
 - Son más costosos que otros métodos.

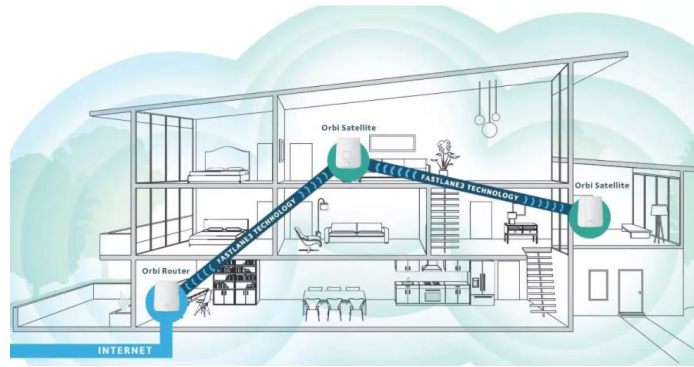


Figura 3-35 Red Mallada (Mesh) [80]

- **Conexión Ethernet** [81]: Es una variante de la red mallada (mesh) ya que permite la conexión entre los distintos puntos de acceso que se configuran en una misma red. En este caso la comunicación entre los puntos de acceso maestros y esclavos se produce a través de un enlace Ethernet.

Las principales ventajas e inconvenientes de este método son los siguientes:

- Ventajas:
 - Mayor velocidad real de la conexión WiFi.
 - Mayor estabilidad de las conexiones.
 - Menos saturación de la red WiFi, lo que redundará en la velocidad y estabilidad de la red.
 - Menor latencia y “jitter” [82].
- Inconvenientes:
 - El firmware del punto de acceso debe disponer de esta funcionalidad.

Una vez valorados los pros y contras de los tres métodos descritos anteriormente se va a desplegar la red WiFi en base a un despliegue Ethernet con el objeto de conseguir la máxima velocidad y estabilidad de la red y de mejorar la saturación radio de la zona de cobertura.

3.8.3 Despliegue de la red

Como anteriormente se ha citado, para el despliegue de la red se va a utilizar un punto de acceso maestro (AP1) y dos puntos de accesos esclavos (AP2 y AP3), mediante una arquitectura en modo infraestructura (figura 3-36). Este modo es el método más comúnmente utilizado en pequeñas empresas, hogares y oficinas.

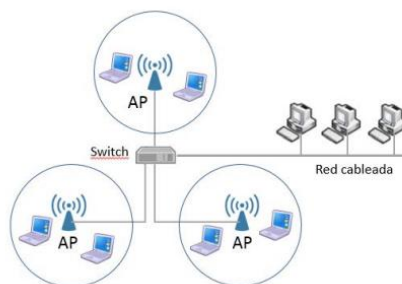


Figura 3-36 Diagrama de una red inalámbrica modo infraestructura [35]

En el caso de estudio el diagrama de instalación y de las conexiones se muestra en las figuras 3-37 y 3-38 respectivamente:

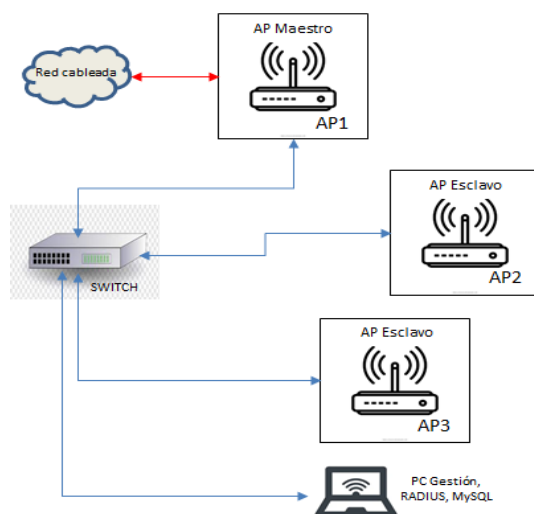


Figura 3-37 Diagrama de la instalación (elaboración propia)

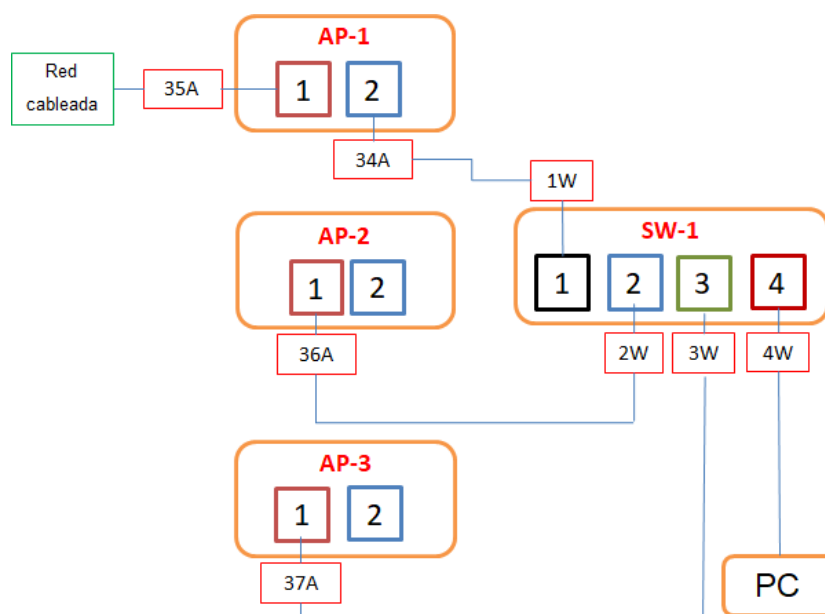


Figura 3-38 Diagrama de conexiones (elaboración propia)

En la tabla 3-02 con las conexiones establecidas:

Rúter	Salida		Destino	
	Nº	Toma	Nº	Toma
AP1	1	35-A		Red cableada
	2	34-A	1W	Switch
AP2	1	36-A	2W	Switch
AP3	1	37-A	3W	Switch
PC			4W	Switch

Tabla 3-02 Cuadro de conexiones (elaboración propia)

3.8.4 Asignación de direccionamiento IP

El objetivo del direccionamiento IP es identificar de forma inequívoca a cada dispositivo de la red. Por lo tanto, es un número que identifica a una interfaz, que puede ser un punto de acceso, un dispositivo cliente, etc.

La asignación de la dirección IP puede ser de forma estática o dinámica. En el primer modo el administrador de la red asigna la dirección IP a cada dispositivo dicha dirección IP no varía de forma automática. Esta modalidad estática se asigna a dispositivos que necesitan conocer y ser conocidos de manera continua, por ejemplo, los puntos de acceso, servidor RADIUS, etc. La asignación dinámica es la modalidad de asignación de dirección IP que se asigna a dispositivos que no necesitan ser localizados de manera continua, por ejemplo, los dispositivos de usuario.

Esta asignación normalmente es misión del servidor DHCP (protocolo de configuración dinámica de Host).

Por lo tanto, según lo anteriormente expuesto las asignaciones a la red WiFi planteada son las que se muestran en la tabla 3-03:

Parámetros del servidor DHCP		
Servidor DHCP	Enable	
DHCP Start IP Address	192.168.1.2	
DHCP End IP Address	192.168.1.100	
Assign DNS	Enable	
DNS Server IP Address	208.67.222.222	
Default Gateway	192.168.1.1	

Allocated Address		
MAC	IP	HOST NAME
00:a0:65:c3:2d:ab	192.168.1.3	AP1
00:30:6e:00:15:97	192.168.1.4	AP2
08:00:11:12:8c:b7	192.168.1.5	AP3
00:0b:db:85:50:b9	192.168.1.6	RADIUS
00:60:08:76:c1:e4	192.168.1.7	MySQL
00:85:6e:15:ab:08	192.168.1.8	PC Gestión

Tabla 3-03 Direccionamiento IP (elaboración propia)

3.9 Bastionado de la Red WiFi

En este momento los puntos de accesos se hayan radiando y por tanto los posibles clientes están en condiciones de establecer una comunicación WiFi a través de ellos. La configuración de fábrica de los puntos de acceso y la configuración realizada posteriormente sobre el gestor de configuración web están proporcionando una seguridad mínima sobre la infraestructura. No obstante, y según lo expuestos en los puntos 3.4 “*Determinación del nivel de seguridad de la red inalámbrica corporativa*” y 3.5 “*Requerimientos de seguridad de la red inalámbrica corporativa*”, la red inalámbrica planteada en este proyecto necesita de un nivel de seguridad adicional que la permita adaptarse a lo especificado en la guía CCN-STIC-804 “*Medidas de implantación del ENS*”.

En los apartados posteriores se va a proceder a la configuración adicional de seguridad que permita a la red corporativa proteger la información sensible que circula por ella. No obstante los datos de acceso a la misma, previos a su bastionado, son los siguientes:

- Wireless 1 (red corporativa):
 - Cifrado: WPA2, PSK y AES.
 - Contraseña acceso: j9sxTwrhFyhz3CKYlQN4
 - SSID: TFM2021

Respecto a la red de invitados, actualmente se encuentra activa con una seguridad mínima compuesta por el SSID con los datos de enlace siguientes:

- Wireless 2 (red invitados):
 - Cifrado: WPA+WPA2, PSK y AES
 - Contraseña de acceso: UPC-Invitados
 - SSID: UPC-Invitados

Los datos referentes a la red de invitados proporcionarán a los clientes acceso a red pero no a sus recursos. Tras la acreditación ante la red los clientes serán transferidos a un portal de acceso donde se les informará de la normativa de protección de datos vigente y se les requerirá otra acreditación basada en su documento nacional de identidad y de la contraseña suministrada por la Universidad (figura 3-39).



Figura 3-39 Acceso a la red de invitados [elaboración propia]

Para adaptar la red corporativa a la guía CCN-STIC-804 “*Medidas de implantación del ENS*” se van a realizar las siguientes medidas de seguridad:

- Disponer de un sistema de autenticación.
- Cambiar el puerto de acceso al router:
 - Realizado previamente a través de la configuración web.
 - Se ha deshabilitado el acceso a través de Telnet y HTTP, dejando como únicos medios de acceso a la administración de los puntos de acceso el acceso vía SSH y HTTPS.
 - Así mismo, se ha modificado el puerto de acceso por defecto de SSH (22) por el puerto 1024.
- Uso canales menos saturados:
 - Se ha configurado el punto de acceso para la búsqueda y uso automático de canales menos saturados.
- SSID oculto:
 - Se ha deshabilitado la publicación abierta del SSID de la red corporativa.
- Añadir una contraseña de cifrado para WPA2:
 - Se ha configurado el método de cifrado en la configuración previa, añadiendo una contraseña de cifrado.
- Deshabilitar WPA y TKIP:
 - Medida realizada en la configuración vía web.
- Filtrado de red a través de MAC:
 - Medida implementada a través de la configuración vía web.

Una vez hecha la configuración vía HTTPS, la otra vía de acceso es vía SSH. Para acceder por esta SSH se podría usar el software PuTTY (figura 3-40). PuTTY es un cliente SSH (Telnet, Rlogin y TCP raw) de licencia libre, disponible para el sistema operativo Windows y plataformas Linux.

Mediante este software se crea un túnel encriptado entre el PC gestor de configuración y el router remoto iniciando una sesión segura entre ellos que permite ejecutar comandos de configuración.

PuTTY tiene las siguientes características:

- Es gratuito y de código abierto.
- Disponible en varias plataformas (Linux y Windows).
- Almacena el historial de conexiones anteriores y sus preferencias para posteriores usos en futuras sesiones.
- Soporte 3DES, AES, RC4, DES Blowfish.
- Soporte de autenticación con clave pública.
- Muestra la respuesta de los puertos requeridos.
- Soporte para IPv6.
- Soporte para SCP (*Secure Copy Protocol*) y SFTP (*Secure File Transfer Protocol*).

Otra opción de conexión a través de un túnel SSH sería a través de Windows 10 que dispone de su propio cliente y servidor SSH basado en OpenSSH.

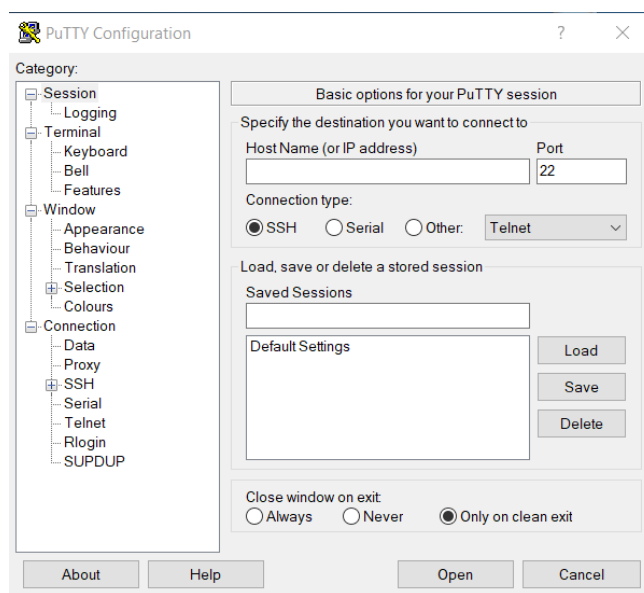
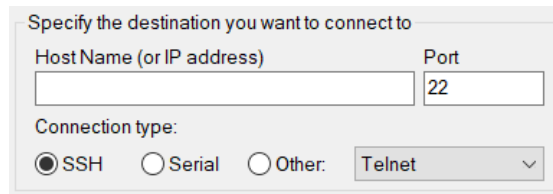


Figura 3-40 Consola de PuTTY [98]

Sin entrar en detalles descriptivos de la aplicación PuTTY que se excederían de ámbito de este trabajo, PuTTY presenta la interfaz mostrada en la figura 3-40, en la cual realizaríamos las siguientes acciones para acceder al router:

- *Host Name* (or IP address): Se introduce la IP del router (192.168.2.1) o el nombre del router (AP1, AP2 o AP3) (figura 3-41).
- *Port*: Indica el puerto a través del cual se va a realizar la conexión al router. El puerto tradicional es el 22, aunque ha sido modificado por el puerto 1024.
- *Connection type*: De las 5 opciones que se muestran solo se usará SSH. Telnet era una opción válida hace unos años pero hoy en día se considera un medio no seguro

ya que todos los nombres de usuario y contraseñas viajan por la red en forma de texto plano y por tanto son vulnerables.



Specify the destination you want to connect to

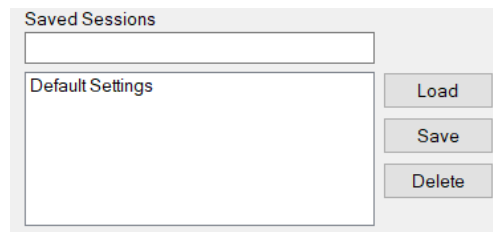
Host Name (or IP address) Port

Connection type:

☒ SSH ☐ Serial ☐ Other:

Figura 3-41 Extracto superior consola de PuTTY [98]

Los datos que se introduzcan pueden guardarse para futuras conexiones en el apartado “Saved Sessions” (figura 3-42):



Saved Sessions

Default Settings

Figura 3-42 Extracto inferior consola de PuTTY [98]

Con los datos arriba indicados se accede a una consola en la cual introducimos las credenciales de acceso (figura 3-43):



192.168.1.2 - PuTTY

```
login as:
root@192.168.1.2's password: 
```

Figura 3-43 Acceso a credenciales PuTTY [98]

3.9.1 Control acceso de usuarios

Según la ISO 27001 [83], los controles de acceso otorgan a los usuarios autorizados el derecho a acceder a un servicio o a una información, en tanto que se impide el acceso a otros usuarios no autorizados.

El Anexo A.9.I de la ISO 27001 [83] dice lo siguiente *“Los usuarios sólo deben tener acceso a la red y a los servicios para los que se les ha autorizado específicamente para usar. El acceso debe ser controlado por un procedimiento de inicio seguro y restringido, de acuerdo con la política de control de acceso”*.

El control de acceso a la red es una medida básica en todos los estándares de seguridad y garantiza que el usuario que pretende acceder a la red tiene las credenciales necesarias para ello y que una vez dentro de la red se le suministran exclusivamente los privilegios necesarios para realizar su función.

La guía CCN-STIC 804 *“Medidas de implantación del ENS”* establece en el punto 4.2.5 *“[OP.ACC.5] Mecanismo de autenticación”* la obligatoriedad de que exista un mecanismo que permita validar la identidad del usuario.

Típicamente los mecanismos de autenticación recurren a:

- Algo que se conoce (un secreto, por ejemplo, una contraseña).
- Algo que se tiene (un objeto, por ejemplo, una tarjeta o una llave).
- Algo que es propio del usuario (características biométricas).

Comúnmente estos mecanismos se emplean combinados en busca de dificultar la falsificación de los mismos. Por ejemplo:

- Una tarjeta y un número secreto.
- Una tarjeta y una huella dactilar.
- La huella dactilar y una contraseña

Cada mecanismo tiene sus debilidades y sus fortalezas. No obstante, ninguna medida es infalible a los ataques. Las medidas técnicas deben completarse con normativas y procedimientos que regulen su uso, periodo de validez y gestión de incidencias en caso de pérdida o descubrimiento.

Las credenciales deben estar bajo el control efectivo del usuario y ser exclusivas del mismo, prohibiéndose su divulgación no segura o el uso compartido de credenciales a un grupo de usuarios. Las credenciales facilitan la trazabilidad de acciones en la red. En el caso, que tras un incidente de seguridad o robo de información se deba rastrear al usuario responsable, las credenciales podrán identificar al mismo, en el caso de credenciales compartidas dicho señalamiento sería imposible.

Otra medida básica de seguridad en el uso de credenciales es el establecimiento de medidas de seguridad en la periodicidad de su caducidad, su complejidad y su repetición temporal. La organización deberá establecer dichas medidas en sus políticas de seguridad. Así mismo, las mismas políticas de seguridad deben establecer medidas para aquellos usuarios que finalicen su necesidad de uso de las credenciales tras el fin del periodo de relación con la red o tras un periodo de no inactividad en la red.

Existen diferentes opciones comerciales para proteger a la red del acceso no autorizado de usuarios o posibles atacantes. Algunas opciones están orientadas a nivel profesional para grandes empresas con gran cantidad de usuarios (NAC) y otras para redes más modestas con un número de usuarios más reducido. En la red corporativa de este proyecto y debido al número red de usuarios se optará por un sistema de control de acceso que proporcione la adecuada seguridad en relación a la información que queremos proteger. Por lo tanto, se optará por un sistema bastante conocido llamado RADIUS.

3.9.2 Servidor de autenticación RADIUS

RADIUS (*Remote Authentication Dial-In User Server*) [84] se trata de un protocolo de autenticación y autorización para aplicaciones de acceso red.

El servidor de autenticación RADIUS estará virtualizado en el PC de gestión, el cual también ubicará la base de datos y el controlador de puntos de acceso.

El proceso de autenticación se inicia cuando el cliente se conecta al punto de acceso WiFi a través de las credenciales correspondientes. El punto de acceso remitirá las credenciales del cliente al servidor RADIUS. El servidor comprueba la información, contrastándola con la base de datos (MySQL). Si el usuario es aceptado el servidor le dará el acceso al sistema, asignándole los recursos de red necesarios para establecer la conexión a la misma, tales como IP, puerta de enlace, etc. Si las credenciales no son correctas el servidor rechazará la conexión.

Previamente a la configuración del servidor RADIUS, hay que diferenciar cliente, usuario y servidor:

- Servidor es el lugar donde se procesan las solicitudes de acceso.
- Cliente es el rúter al que se solicita el acceso.
- Usuarios son los clientes que solicitan acceso al rúter.

Para configurar el servidor RADIUS se accederá a la configuración web, se rellenará la dirección IP del servidor RADIUS primario, existe la opción de un segundo servidor, indicando el puerto de enlace y el secreto compartido por el punto de acceso y por el servidor RADIUS.

Otra opción es acceder al servidor RADIUS vía SSH y configurar los ficheros que no se ajusten a la configuración deseada. Los archivos modificables son los que figuran en la tabla 3-4:

Radius.conf	Con referencia al resto de archivos de configuración, define los parámetros de configuración del servidor.
Cientes.conf	Define la información para configurar al cliente RADIUS, incluyendo direcciones IP y los secretos compartidos (código que debemos introducir en la propia configuración del rúter cliente).
Dictionary	Hace referencia a los atributos de diccionarios por defecto.
Proxy.conf	En caso de existir, define el servidor principal que daría servicio a servidores secundarios.
Sites-enabled/default	Servidor virtual por defecto. Maneja las peticiones de contabilización y autenticación.
Sites-enabled/inner tunne	Es un servidor virtual que gestiona los métodos de autenticación que son remitidos vía túnel TLS.
Users	Es el archivo de configuración de los propios usuarios de RADIUS

Tabla 3-4 Configuración servidor RADIUS (elaboración propia)

A continuación se procede a variar aquellos parámetros específicos de nuestra red (tabla 3-5):

Clients.conf	Se añaden clientes nuevos al servidor. Los clientes se definen por su IP y por su secreto (figura 3-44)
Users	Este archivo nos permite asignar un nombre de usuario y una contraseña a cada uno de los dispositivos autorizados a acceder a la red. Esto también nos permite revocar el acceso de usuarios caducados o revocados sin tener que modificar los parámetros comunes al resto de los usuarios

Tabla 3-5 Configuración específica servidor RADIUS (elaboración propia)

RADIUS también nos permiten implementar una serie de modificaciones que podrían ser de utilidad, tales como la limitación de conexiones simultáneas o el tiempo máximo de conexión por usuario, opciones que también pueden ser definidas por el punto de acceso (figura 3-45).

```
client new {
    ipaddr =
    secret =
```

Figura 3-44 Nuevo usuario servidor RADIUS (elaboración propia)

```
Usuario_1 Cleartext-Password :=
Simultaneous-Use := 1
```

Figura 3-45 Limitación de conexiones simultáneas (elaboración propia)

Una vez configurado el servidor, procedemos a la configuración del cliente, para ello accederemos a la configuración wireless que se muestra en la figura 3-20. Algunos parámetros ya estarán configurados previamente desde la consola web (tabla 3-6):

encryption	Previamente configurado. Encriptación WPA2+CCMP, sin posibilidad de uso de TKIP
auth_server	Previamente configurado. IP en la que se encuentra el servidor RADIUS (tabla 3-03)
auth_secret	Se añade el “secreto” que comparten el servidor RADIUS con sus clientes
acct_server	Se añade la IP en la que se encuentra el servidor de monitorización de usuarios
auth_port	Puerto de enlace predeterminado por RADIUS como puerto de utenticación, 1812
acct_port	Puerto de enlace predeterminado por RADIUS como puerto de contabilización, 1813

Tabla 3-6 Configuración cliente RADIUS (elaboración propia)

Con estas configuraciones se habrá configurado el servidor de autenticación RADIUS, no obstante dicho servidor necesita una base de datos para la gestión de los usuarios.

3.9.3 Configuración de la base de datos

La base de datos es el lugar donde el servidor RADIUS acudirá para comprobar que las credenciales de los usuarios que pretenden entrar en la red son correctas o incorrectas. El uso de una base de datos facilita la creación, modificación y borrado de usuarios.

En la base de datos se reemplazará los archivos *users* y *clients.conf*.

Para ello se necesita descargar el paquete “*mysql-apt-config 0.8.20-1_all.deb*”. Se cargan los archivos y se instalan a través del comando “*\$ sudo dpkg i ~/Descargas/mysqlapt-config 0.8.20-1_all.deb*”.

Una vez instalado MySQL se procede a configurar la base de datos para trabajar conjuntamente con RADIUS, para ello crearemos una base de datos específica en MySQL.

Creación de una base de datos MySQL:

- Se lanza el servidor MySQL.
- Se comprueba el estado del servidor MySQL a través del comando “*sudo service mysql status*”.
- En caso de que esté apagado se encenderá con el comando “*sudo service mysql start*”.
- Se accede al motor del servidor MySQL a través del comando “*\$ mysql -uroot -p*”.
- Una vez en el motor del servidor creamos nuestra base de datos específica, en nuestro caso se llamará “*radius*”, *mysql > create database “radius”*.
- Se importan las tablas y configuraciones que trae el servidor RADIUS para su uso en MySQL, “*mysql > source radius*”. (figura 3-46).
- Se importa el fichero “*schema.sql*” a través del comando “*source*”.

- Es posible que las tablas importadas tengan la estructura definida pero que carezcan de datos. Es necesario rellenar las tablas *NAS* y *RADCHKET*, que son las tablas que reflejan los clientes conectados a RADIUS y los usuarios con autorización de acceso a la red (figura 3-47).
- Para rellenar las tablas que interesan se aplica el comando *insert into nombre de la tabla (valores)*. Por ejemplo:” *insert into radcheck (username.attribute.op.value) values “Usuario1”. “Cleartext-Password”, “=”, “madrid”);*
- Una vez configurada la base de datos MySQL se procede a configurar el servidor RADIUS para que en vez de usar los archivos “*users*” y “*clients.conf*” use la base de datos recién creada:
 - *radiusd.conf*: Se modifica este archivo para añadir “*\$includemods.enabled/*” en “*modules* y *\$includesites-enabled/* *enpolicy*” (figura 3-48).
 - *default*: Modificamos este archivo activando *SQL* en todos los apartados.
 - *../mods-available/*: Se cambiarán los parámetros de conexión a la base de datos en esta carpeta, teniendo en cuenta que los parámetros mostrados (figura 3-49):
 - *Driver*: mysql.
 - *Dialect*: mysql.
 - *Server*: IP en la que se encuentra el servidor RADIUS.
 - *Port*: Puerto de conexión, 3306.
 - *Login*: Usuario con permiso de acceso a la base de datos.
 - *Password*: Contraseña de acceso a la base de datos.
 - *Radius.db*: Indica qué base de datos de todas las disponibles del servidor SQL que se debe emplear “*radius*”. En este archivo se añadirá “*read_clients=yes*” para leer los clientes de la base de datos y “*client_table=“nas”*” para indicar que tabla debe leer para seleccionar los clientes.

Con estos cambios estaría acabada la configuración de la base de datos MySQL para su uso conjunto con RADIUS. Por último, se verifica si la configuración es correcta con el comando “*\$ sudo radius -XC*”, si todo está correcto devolverá el mensaje “*configuration appears to be OK*”.

```
mysql> use radius
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> source /etc/freeradius/3.0/mods-config/sql/main/mysql/schema.sql
Query OK, 0 rows affected (0,89 sec)

ERROR 1050 (42S01): Table 'radcheck' already exists
Query OK, 0 rows affected (0,35 sec)

Query OK, 0 rows affected (0,36 sec)

ERROR 1050 (42S01): Table 'radreply' already exists
Query OK, 0 rows affected (0,35 sec)

Query OK, 0 rows affected (0,30 sec)

Query OK, 0 rows affected (0,32 sec)

mysql>
```

Figura 3-46 Importación de tablas de RAD (elaboración propia)

```
mysql> SHOW TABLES;
+-----+
| Tables_in_radius |
+-----+
| nas               |
| radacct           |
| radcheck          |
| radgroupcheck     |
| radgroupreply     |
| radpostauth       |
| radreply          |
| radusergroup      |
+-----+
8 rows in set (0,00 sec)

mysql>
```

Figura 3-47 Tablas base datos MySQL (elaboración propia)

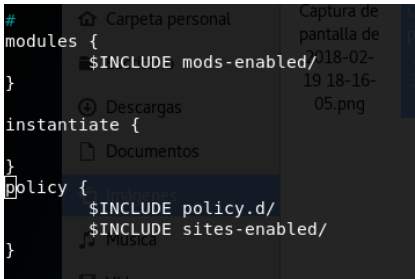


Figura 3-48 Configuración radius.conf
(elaboración propia)

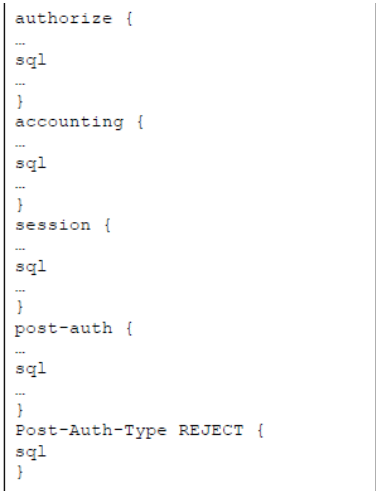


Figura 3-49 Configuración siterr.available
(elaboración propia)

Para la gestión y configuración de la base de datos existen diferentes opciones que facilitan dicha labor, una de ellas es *MySQL Enterprise Monitor* (figura 3-50). Dicha aplicación permite a través de un interfaz “amigable” el acceso a los servidores MySQL disponibles, tablas disponibles y modificación de las mismas.

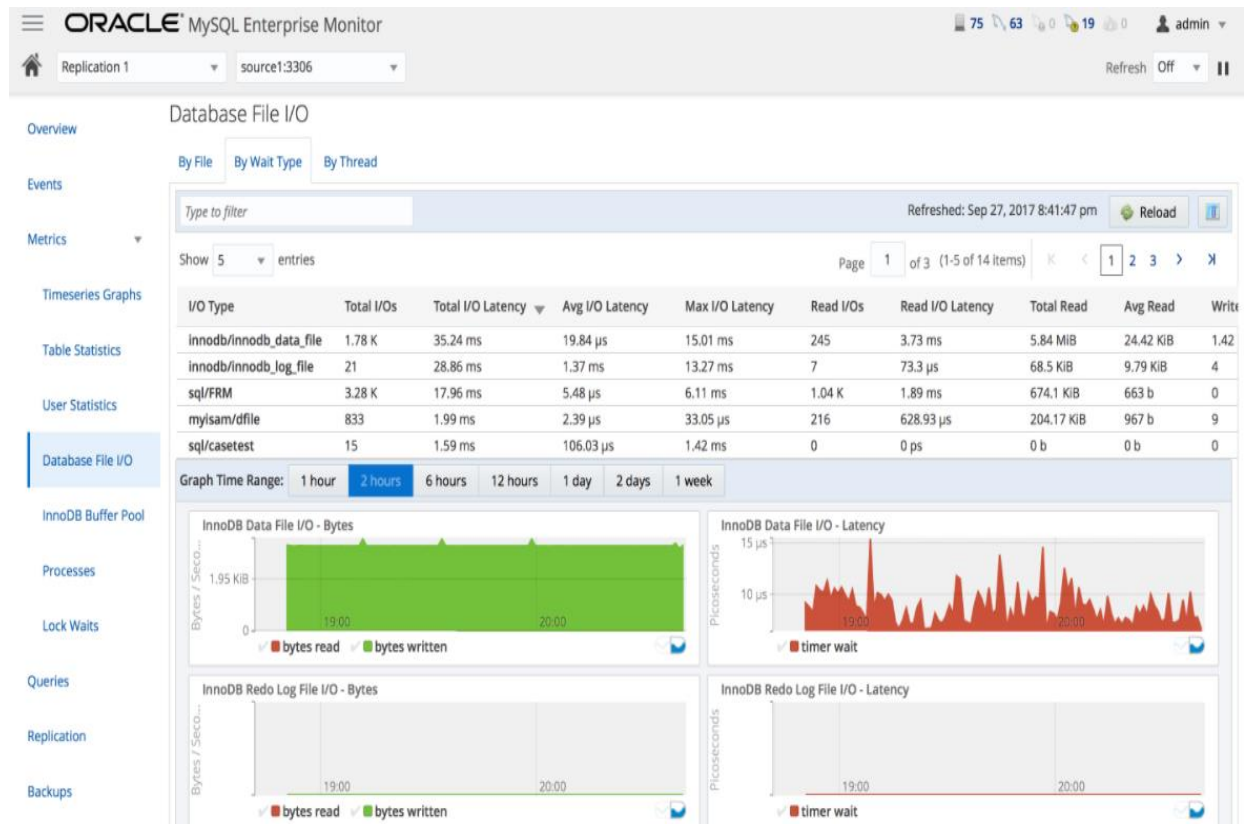


Figura 3-50 MySQL Enterprise Monitor [85]

3.9.4 Sistema de detección de Intrusos

Una vez instalada, configurada y securizada la red el último paso que queda para adaptar la misma a la normativa en vigor la guía CCN-TIC-816 “*Seguridad en Redes Inalámbricas*” [86], es dotarla de un sistema de detección de intrusos.

Un Sistema de Detección de Intrusos (IDS) o un Sistema de sistema de Prevención de Intrusiones (IPS) [89], son una clase de software ideada para detectar o prevenir accesos no autorizados a un equipo o red, para ello monitorizan el tráfico entrante y lo comparan con una base de datos de firmas de ataques conocidos. En el caso de que haya coincidencia con la base de datos de ataques el IDS emitirá una alarma que deberá ser investigada por el personal de seguridad correspondiente. A diferencia de los IDS, los IPS no solo emiten una alarma visible para los operadores de seguridad, sino que realizan una acción previamente determinada por estos.

Los sistemas IDS/IPS tienen su versión para redes inalámbricas [87], denominándose WIDS (Wireless IDS) o WIPS (Wireless IPS) y suelen estar compuestos por los siguientes elementos (figura 3-51):

- **Sensores:** Son los dispositivos que monitorizan y capturan la actividad de la red. Pueden ser:
 - **Dedicados:** Son dispositivos independientes dedicados únicamente a la función de sensor.
 - **No dedicados:** El sensor es una función integrada en otro dispositivo de la red inalámbrica. Por ejemplo, en el punto de acceso o en conmutadores.
 - **Software en el dispositivo cliente:** Es un software que se instala en el equipo cliente. Tiene la función de detectar ataques o vulnerabilidades y enviar esa información a los Servidores de Administración.
- **Servidores de Administración:** Son los equipos que analizan la información enviada por los sensores.
- **Servidores de Base de Datos:** Son los equipos que almacenan los eventos generados por los Servidores de Administración. Se tiene que tener en cuenta aspectos legales que obligarán a almacenar dichos registros por un periodo determinado.
- **Consola:** Es el interfaz de gestión y control del sistema.

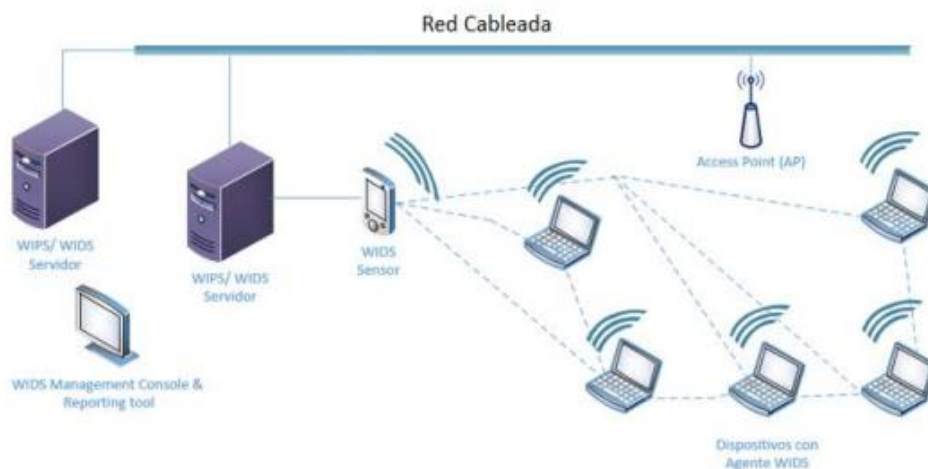


Figura 3-51 Arquitectura de un Sistema WIDS/WIPS [86]

En el caso que nos ocupa el sistema WIDS/WIPS tendrá la misma cobertura que la red inalámbrica, con el objeto de que individuos no autorizados se ubiquen en zonas donde puedan eludir al sistema de detección.

Los accesos sospechosos pueden ser ataques esporádicos realizados por usuarios externos malintencionados buscando posibles víctimas o pueden ser realizados por los propios usuarios legítimos debido a desconocimiento o a actos de sabotaje en la misma red (*Insiders*) [87]. En cualquier caso, toda actividad ilícita o sospechosa debe ser registrada e investigada para evitar fugas de información no deseadas o para detectar vulnerabilidades que pongan en riesgo la información a proteger.

Obviamente, del uso de soluciones tipo IDS/IPS surge la necesidad imperiosa de mantener la base de datos de amenazas constantemente actualizada, en caso contrario los ataques pasarán desapercibidos para el IDS/IPS.

El sistema de detección puede estar integrado en la misma red o ser parte un sistema de detección más amplio. En este caso, deberíamos instalar un sensor o sonda en nuestra red que reportase eventos a un servidor de eventos que a su vez los va a correlacionar con un listado de reglas de seguridad del mismo e informaría a un elemento superior tipo SIEM (*Security Information and Event Management*) [88].

La red corporativa del proyecto es relativamente pequeña y el número de clientes de la misma no va a ser en ningún caso elevado. Por lo tanto, la opción de la supervisión de eventos externa es la más práctica. No obstante, para completar este trabajo y mostrar la instalación y configuración de un IDS (*Intrusión Detection System*) se va a contar con un IDS tipo comercial adaptado a redes inalámbricas.

El número de IDS disponibles en el mercado es amplia, tanto en su faceta de pago como gratuita, no obstante, se ha optado a instalar en la red inalámbrica de estudio el IDS llamado Kismet debido a que sus características se adaptan mejor a redes WiFi.

Sistema de Detección de Intrusos Kismet

Kismet [89] es un software basado en Linux que permite monitorizar redes inalámbricas (WLAN).

Sus principales funciones son:

- Verifica que nuestra red está bien configurada.
- Detecta redes externas que puedan perturbar a nuestra red.
- Detecta puntos de acceso colindantes a nuestra red.
- Nos muestra información relativa a los clientes conectados a la red.
- Nos indica el tipo de protección que tenemos activada (WEP, WPA, WPA2, etc).
- Proporciona información sobre los canales utilizados e intensidad de señal.
- Funciona en forma monitor, guardando en un archivo de texto los paquetes capturados. Este aspecto es fundamental para un posterior análisis forense.

En realidad, Kismet es un rastreador de redes inalámbricas que recopila información sobre las WLAN disponibles, los puntos de acceso, clientes y canales de transmisión utilizados, siempre funcionando de forma pasiva.

Esta manera de trabajar hace a Kismet idóneo para:

- Actuar como IDS.
- Facilitar revisiones de seguridad.

- Realiza inventario de activos.
- Búsqueda sistemática y mapeo de la red.

En la red corporativa del proyecto se usará exclusivamente como IDS, para ello deberemos instalar un servidor y un cliente Kismet en nuestro equipo y un sensor en el punto de acceso que se vaya a habilitar como monitorizador de la red.

Para la instalación de Kismet se seguirán los siguientes pasos:

- **Instalar Kismet en el terminal de usuario:** Kismet es una aplicación creada para sistemas basados en Unix (Linux, OS X, FreeBSD, NetBSD, OpenBSD), aunque también es posible su instalación en Windows a través de CYGWIN (colección de herramientas para proporcionar un comportamiento similar a los sistemas Unix en Windows). Recurriremos a la distribución Kali Linux que ya trae instalada una versión Kismet como herramienta nativa. No obstante, en caso necesario de instalar Kismet en Linux se realizaría a través del comando “\$ sudo apt-get install kismet”.

Esta preinstalación lo normal es que no funcione, ya que se tendrán que variar algunos parámetros del archivo “*kismet.conf* ubicado en */etc/kismet*”. Para ello, se ejecutará el comando “*sudo pluma /etc/kismet/kismet.conf*”.

En el archivo *kismet.conf* aparecerán todas las líneas con el signo # al inicio de las mismas, eso significa que el intérprete las pasará por alto, lo que es una manera de mantener opciones desactivadas y de fácil activación posterior con solo quitar el signo #.

En este caso, se va a capturar la información que nos va a mandar una sonda instalada en un punto de acceso. En Kismet estas sondas se llaman “drones”, por lo tanto, se va a modificar el archivo *kismet.conf* para que reciba la información del dron.

Esta configuración se hará según los siguientes pasos:

- Acceder vía SSH al punto de acceso elegido.
- Lanzar el comando “*nsourse=drone:host=192.169.1.3, port=2502*”, con este comando se está indicando que el interfaz elegido es un dron, cuya IP y puerto son los del rúter en el que se va a instalar.
- **Instalación del dron Kismet:** Una vez se ha accedido al rúter correspondiente se procede a teclear los siguientes comandos (figuras 3-52 y 3-53):

```
root@Router3: ~# opdk update
```

Figura 3-52 Actualización del repositorio opdk (elaboración propia)

```
root@Router3: ~# opkg install kismet-drone
```

Figura 3-53 Instalación del dron Kismet (elaboración propia)

Si la instalación ha sido correctamente completada en la carpeta */etc* debe aparecer una carpeta con el nombre de *Kismet* (figura 3-54).

```
ls
hotplug2-common.rules  preinit
hotplug2-init.rules   profile
hotplug2.rules        protocols
init.d                rc.common
inittab               rc.d
kismet                rc.local
modules.d             resolv.conf
mtab                  services
nixio                 shells
openwrt_release       sysctl.conf
openwrt_version       sysupgrade.conf
opkg.conf             uci-defaults
passwd
```

Figura 3-54 Extracto de la carpeta /etc con el dron kismet creado (elaboración propia)

Se accede al directorio Kismet y muestra el contenido del fichero “*kismet_drone.conf*”. Dentro de este fichero se añade el nombre que le vamos a dar al servidor kismet-Drone y le indicamos con la opción “*dronelisten=tcp://192.168.1.3:2502*” la dirección IP a la cual se han de conectar los dispositivos para leer la información disponible, así como el puerto 2502.

En la línea “*droneallowedhost=127.0.0.1,192.168.1.200*”. Se le indica al dron quien puede conectarse a él para leer los datos.

Le indicamos que monitorice la interfaz Wireless 1 del router, y también se debe especificar qué tipo de interfaz monitorizar (figura 3-55).

```
# Name of drone server (informational)
servername=Kismet-Drone

# Drone configuration
# Protocol, interface, and port to listen on
dronelisten=tcp://192.168.1.5:2502
# Hosts allowed to connect, comma separated. May include netmasks.
# allowedhosts=192.168.1.200,10.10.10.0/255.255.255.0
droneallowedhosts=127.0.0.1,192.168.1.200
# Maximum number of drone clients
dronemaxclients=10
droneringlen=65535
# ncsourc=interface:options
ncsourc=wlan0:type=mac80211,prism0,Kismet-Drone
# for example:
```

Figura 3-55 Configuración Drone Kismet (elaboración propia)

Se configura la Wireless 1 como sigue en la figura 3-56:

```
config 'wifi-iface'
option 'device'      'radio0'
option 'network'     'lan'
option 'mode'        'monitor'
option 'ssid'        'Kismet'
```

Figura 3-56 Configuración Wireless 1 (elaboración propia)

Con este último paso se habría configurado el servidor y el dron Kismet, quedaría lanzarlo desde el router, para ello se accede al mismo desde PuTTY, y se ejecuta comando “*kismet_drone*”. En el servidor se lanza el comando “*sudo kismet*” y como resultado mostrará el interfaz de kismet que nos interrogara sobre nuestra intención de lanzar el servidor (figura 3-57):

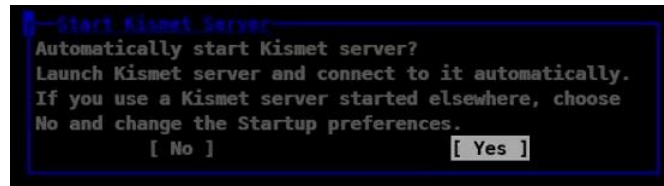


Figura 3-57 Arranque del servidor (elaboración propia)

Al pulsar aceptar primero arrancará el servidor y Kismet empezará a dar información relativa a los puntos de acceso que detecta, otros datos que muestra la consola son los siguientes (figura 3-58).

Los datos de salida que proporciona Kismet son grabados mientras se están ejecutando. Dichos datos generados son almacenados mediante archivos de diferentes tipos:

- ALERT: Archivo de texto que contiene toda la información que Kismet considera extraño.
- GPSMIL: Archivo de texto que guarda las coordenadas de las redes en caso de tener el GPS activo.
- NETTXT: Archivo de texto que guarda la información sobre la red escaneada.
- NETXML: Es la misma información que el archivo NETTXT, pero en formato XML.
- PCAPDUMP: Es el archivo donde Kismet guarda el volcado de memoria. Este fichero puede capturar tráfico desde cualquier analizador de tráfico (TCPDump, Wireshark, etc.) y software como aircrack-ng.

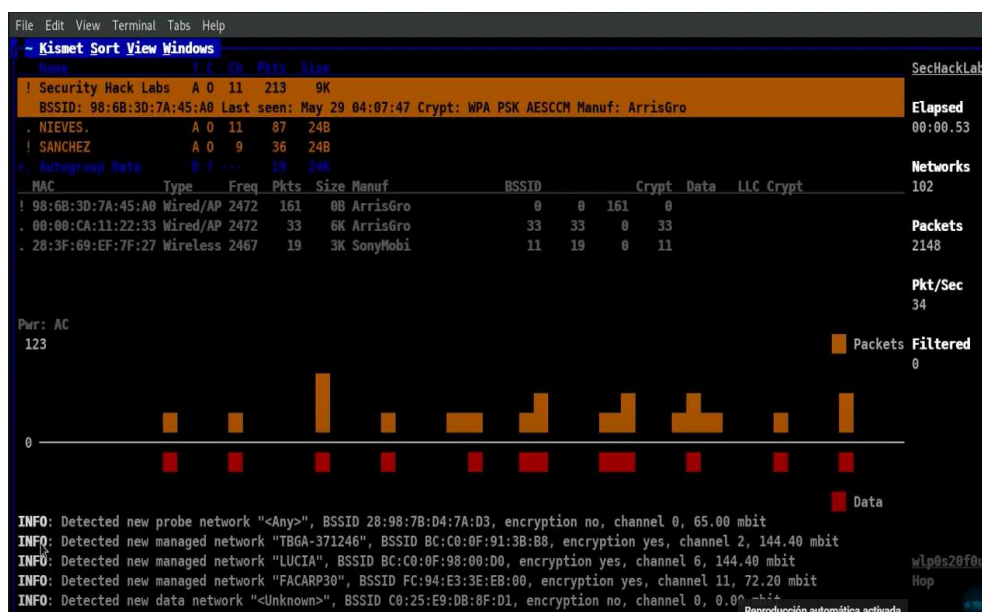


Figura 3-58 Consola Kismet en funcionamiento [92]

Como se indicó anteriormente, una vez configurado el IDS Kismet, este nos enviará información sobre la actividad de la red corporativa. Kismet permitirá al administrador de la red disponer de una herramienta para el control y monitorización de la red.

Al igual que en puntos anteriores, existen soluciones tipo UI que facilitan el uso y configuración de Kismet desde una consola de fácil uso (figura 3-59):

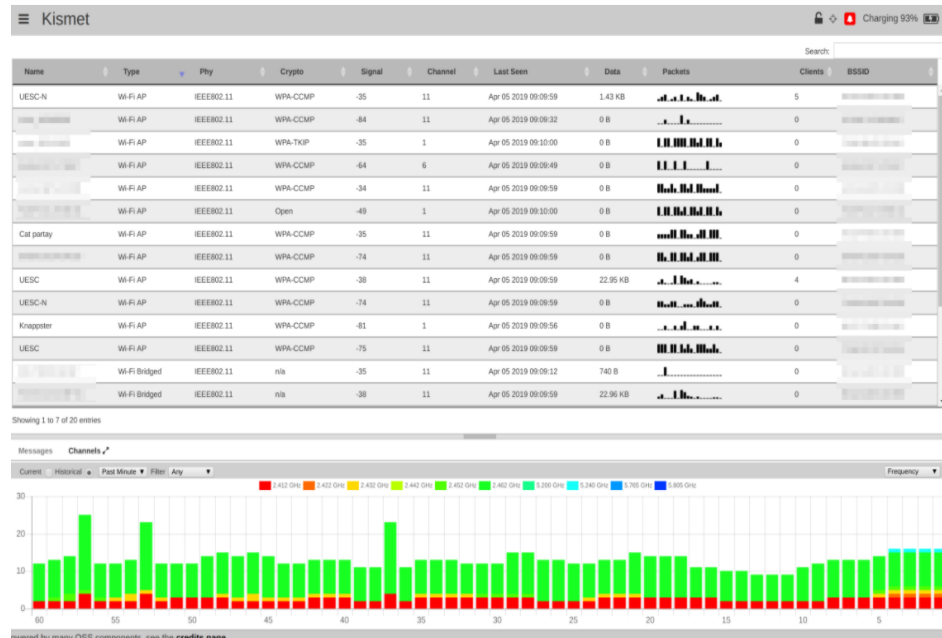


Figura 3-59 Consola Kismet UI [90]

3.10 Acreditación de la Red

Según la guía CCN-STIC-201 “*Organización y Gestión para la Seguridad de las TIC*”, las organizaciones bajo el Esquema Nacional de Seguridad y aquellas que manejen información clasificada de cualquier nivel necesitarán una acreditación para manejar dicha información. Entendiendo por acreditación la “*autorización otorgada a un sistema para manejar información clasificada hasta un grado determinado o en determinadas condiciones de seguridad, con arreglo a su Concepto de Operación*”.

Asimismo, la propia guía CCN-STIC-201, establece que aquellas redes bajo la dependencia del Esquema Nacional de Seguridad (categorías alta, media o baja) y que manejen información sensible o clasificada hasta nivel Difusión Limitada, las inspecciones STIC de acreditación, se delegarán en organizaciones que pueden pertenecer o no al sector privado, denominadas “*Entidades de Certificación (EC)*”.

Por lo tanto, la red corporativa del proyecto deberá pasar previamente a su puesta de funcionamiento un proceso de acreditación que garantice que cuenta con las medidas de seguridad documental, criptográfica, emanaciones electromagnéticas (TEMPEST) y seguridad TIC.

4 PRUEBA Y VALORACIÓN

En este capítulo se mostrará como las medidas de seguridad implantadas según la guía CCN-STIC-816 contribuyen a aumentar el nivel de seguridad de red necesaria según el nivel medio requerido para esta red.

4.1 Medidas implementadas y objetivos alcanzados

En base a los requerimientos de seguridad que establecen las guías CCN-STIC_816 “*Seguridad en Redes Inalámbricas en el ENS*” y en el anexo I de la guía CCN-STIC_803 “*Valoración de los sistemas en Universidades*”, anteriormente citadas en el desarrollo de este TFM, se considera que se han implementado las siguientes medidas de seguridad necesarias para conseguir el nivel de seguridad requerido.

4.1.1 Nivel de seguridad

En base a la normativa en vigor, principalmente las guías CCN-STIC, se ha determinado que el nivel de seguridad apropiado para la instalación es un nivel MEDIO. Dicho nivel es la protección que la información que va a transitar por la red.

No se ha tenido en cuenta la ampliación del nivel de seguridad dentro del Esquema Nacional de Seguridad e incluso por encima del mismo en el caso de que pueda existir información clasificada bajo el paraguas de la Ley de Secretos Oficiales.

Así mismo, se han dado por instaladas las normas de seguridad física pertinentes y necesarias para dotar de protección a los medios de la red instalados. La seguridad física, incluyendo las medidas necesarias para evitar el acceso no autorizado a zonas concretas del edificio, son medidas de gran impacto económico en el proyecto y que cuya materialización ineficiente pone en peligro el resto de medidas de seguridad.

4.1.2 Cobertura del área

Una parte importante del trabajo ha sido el estudio del área de interés, principalmente desde el punto de vista del reparto interno de ubicaciones y por otra parte, los límites que el edificio proporciona y por tanto limitan el área en la cual estamos interesados en dar servicio. A través, de software libre se ha estudiado el área de interés y su composición, decidiéndose las ubicaciones más beneficiosas para la instalación de los puntos de acceso y se ha configurado la potencia de transmisión para que la señal radiada fuera del edificio fuese la mínima.

4.2 Valoración

A continuación se van a realizar una serie de pruebas como validación del procedimiento realizado durante el desarrollo del proyecto. Su objetivo es verificar que las medidas de seguridad implementadas cumplen su función y que proporcionan el nivel de seguridad requerido.

Se han elegido aquellas pruebas más probables de materialización, y para cuya realización se necesita un nivel de conocimientos bajo-medio.

4.2.1 Pruebas de penetración

Las pruebas de penetración o *pentesting* a redes inalámbricas son ataques a un sistema informático con la intención de encontrar las debilidades de seguridad. En el caso que nos ocupa se realizarán ataques a la red inalámbrica con el objeto de detectar aquellas vulnerabilidades que pudiesen suponer una debilidad evidente de la misma.

Las pruebas de penetración suelen concentrarse en el hackeo de la contraseña o el acceso ilegítimo a la infraestructura de la red, en un principio como usuario sin privilegios y posteriormente una elevación de privilegios que permita al atacante conseguir los privilegios de administrador. Las pruebas típicas en las redes inalámbricas abarcan aspectos tales como la identificación de redes ocultas, implementación de un punto de acceso falso, ataques diversos (hombre en medio, denegación de servicio, suplantación de sitios de autenticación, uso de código malicioso e ingeniería social).

En el punto 5.6.2 “*Aceptación y puesta en servicio*” de la guía CCN-STIC_804 “*Medidas de implantación de ENS*”, establece la necesidad de realizar pruebas de penetración como paso previo a la aceptación y puesta en servicio de la red. Dichas pruebas son directamente proporcionales al nivel de seguridad requerido, en el caso de la red corporativa inalámbrica objeto de este trabajo el nivel es MEDIO.

Las pruebas se van a realizar en un ambiente de preproducción por personal adecuado. Dichas pruebas buscan la identificación previa de vulnerabilidades y su salvaguarda, simulando usuarios externos e internos.

La batería de pruebas que se plantean serán las siguientes:

- Identificación de redes ocultas.
- Filtrado de MAC.
- Interfaz segura a través de SSH.
- Romper contraseñas.
- **Prueba de ocultado de SSID.**

Tal y como se ha citado en el desarrollo de este trabajo, el SSID es el nombre identificador de la red. Si bien la ocultación de dicho SSID está destinado a ser una medida de seguridad, lo cierto es que existen numerosas herramientas que detectan y muestran este tipo de redes ocultas. Por lo tanto, el hackeo de esta medida está al alcance de cualquier atacante con un nivel de conocimientos medios/bajos.

NetStumbler, *InSSIDer* y *Kismet*, son algunas de las herramientas que nos permiten levantar la ocultación de las redes WIFI ocultas.

Para la realización de esta prueba se va a utilizar la herramienta InSSIDer, los pasos que se han de realizar son los siguientes (figura 3-60):

- Activar la búsqueda.
- Comparar las redes que InSSIDer descubre con las redes que detecta el controlador WiFi del dispositivo. La diferencia son las redes ocultas.

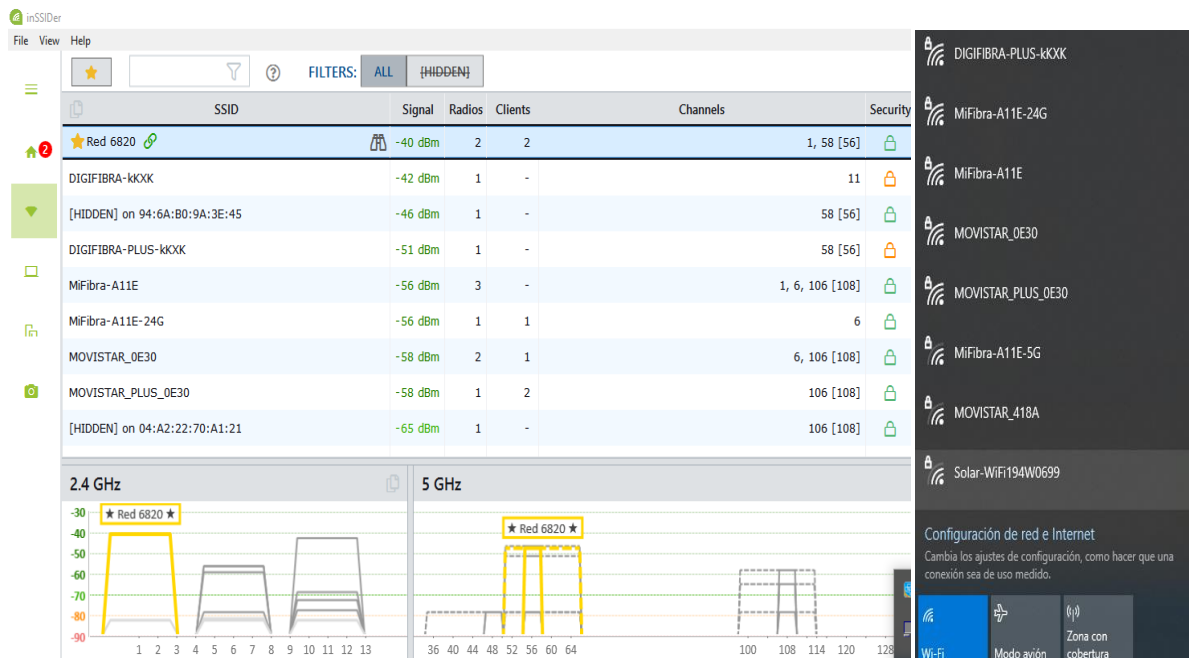


Figura 3-60 Consola InSSIDer (elaboración propia)

• Prueba de filtrado de MAC

Las medida de filtrado de MAC, es una medida fácilmente franqueable por personal atacante con conocimientos medios-bajos. Hoy en día existen multitud de herramientas que permiten solventar estas medidas. No obstante, puede suponer una primera capa de seguridad ante atacantes inexpertos.

Para cambiar la dirección MAC del equipo con el que queremos acceder a la red se empleará el comando “`sudo macchanger mac=00:a0:65:c3:2d:ab Wireless 1`”, según se muestra en la figura 3-61.

```
TFM2021@kali: $ sudo ifconfig Wireless 1 down
[sudo] password for TFM2021:
TFM2021@kali:~$ sudo macchanger -mac=00:a0:65:c3:2d:ab Wireless 1
Current MAC: 0A:00:27:00:00:13
New MAC: 00:a0:65:c3:2d:ab
TFM2021@kali:~$
TFM2021@kali:~$ sudo ifconfig Wireless 1 up
```

Figura 3-61 Suplantación MAC (elaboración propia)

Kismet no detecta el cambio de MAC. No obstante, con un análisis más exhaustivo Kismet sí ha detectado un cambio en un activo de la red como indicio del cambio de MAC. En el caso de que el cambio de MAC se efectuó fuera del área de cobertura de la red, Kismet detectaría dicho cambio sobre una MAC duplicada.

- **Interfaz Web segura a través de túnel SSH**

Para la configuración segura de los puntos de acceso, según la normativa ENS se debe de realizar a través de vías seguras, anulando aquellas otras vías que pueden suponer un riesgo de intrusión en el sistema. Una de las dos vías seguras que el ENS considera seguras es la conexión a través de SSH.

En este caso vamos a realizar dicha conexión SSH a través del Software PuTTY, según se muestra en la figura 3-62.

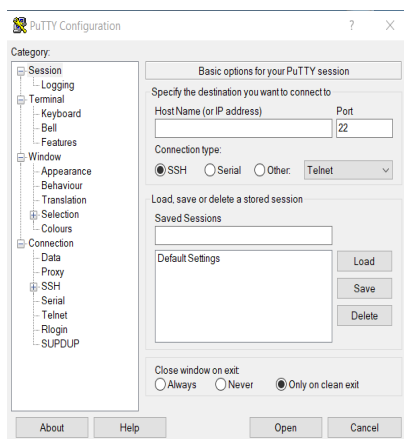


Figura 3-62 Consola Acceso SSH a través de PuTTY [98]

En el caso de acceder al equipo local lo realizaremos a través de la IP local 127.0.0.1:8000. En el caso de que se quiera conectar con un equipo remoto se tendrá que hacer a través de su IP y posteriormente acreditarnos.

Una vez conectados a través de SSH podemos acceder a Wireshark y comprobar que las credenciales de acceso no son visibles y por tanto vulnerables (figura 3-63).

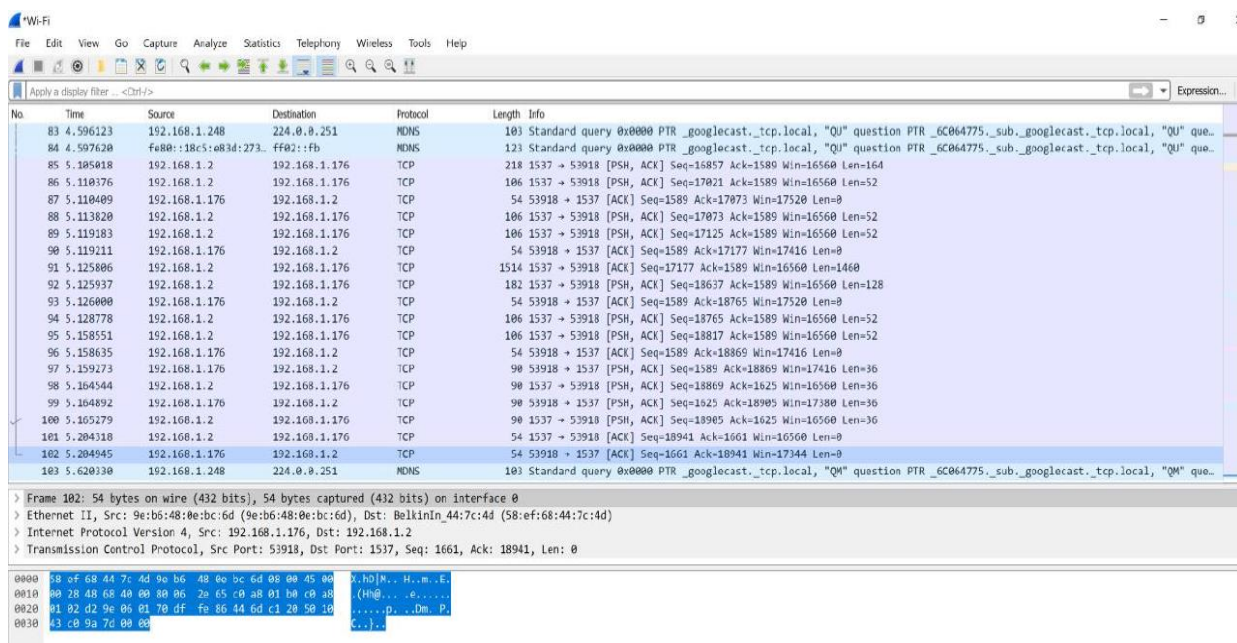


Figura 3-63 Captura de credenciales SSH a través de Wireshark (elaboración propia)

- **Rotura de contraseñas**

- **WPA2 Profesional**

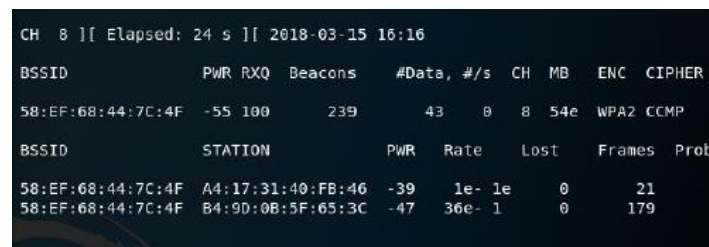
Como se ha citado en el desarrollo de este trabajo una serie de errores en el núcleo del protocolo WPA2 podrían dejar expuestas las conexiones que se realizan a través una red WiFi. Esto permite que el tráfico entre el punto de acceso y sus clientes quede expuesto y aprovechable por un potencial atacante.

El ataque de este tipo más famoso es el ataque KRACK (*Key Reinstallation Attacks*).

Para la realización de esta prueba se utilizará Kali Linux y la aplicación *aircrack-ng* que viene incorporada en Kali Linux.

El proceso del ataque para la realización de la prueba será la siguiente:

- Se monitorizan las redes disponibles, eligiéndose la red Wireless_1.
- Se muestran los clientes conectados.



```
CH 8 ][ Elapsed: 24 s ][ 2018-03-15 16:16
```

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER
58:EF:68:44:7C:4F	-55	100	239	43 0	8	54e	WPA2	CCMP

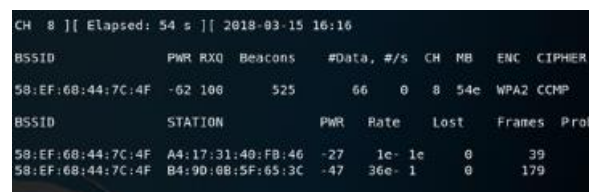
BSSID	STATION	PWR	Rate	Lost	Frames	Prob
58:EF:68:44:7C:4F	A4:17:31:40:FB:46	-39	1e- 1e	0	21	
58:EF:68:44:7C:4F	B4:9D:0B:5F:65:3C	-47	36e- 1	0	179	

Figura 3-64 Interfaz de monitorización Wireless_1 (elaboración propia)

- Se lanza el comando:

```
sudo aireplay-ng -0 2 -a 58:EF:68:44:7C:4F -c B4:9D:0B:5F:65:3C wlan1mon
```

- Deberia aparecer el mensaje con la captura del handshake.



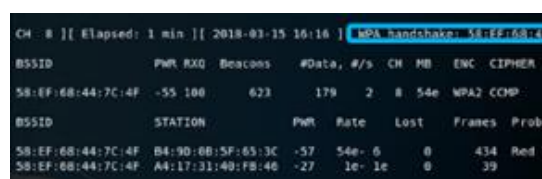
```
CH 8 ][ Elapsed: 54 s ][ 2018-03-15 16:16
```

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER
58:EF:68:44:7C:4F	-62	100	525	66 0	8	54e	WPA2	CCMP

BSSID	STATION	PWR	Rate	Lost	Frames	Prob
58:EF:68:44:7C:4F	A4:17:31:40:FB:46	-27	1e- 1e	0	39	
58:EF:68:44:7C:4F	B4:9D:0B:5F:65:3C	-47	36e- 1	0	179	

Figura 3-65 aireplay-ng ejecutandose (elaboración propia)

- Se debería de proceder a la rotura de la autenticación del cliente, que se volvería a autenticar, haciéndose la captura del handshake. Esta captura se guarda en un archivo tipo .cap.



```
CH 8 ][ Elapsed: 1 min ][ 2018-03-15 16:16 ] WPA handshake: 58:EF:68:44:7C:4F
```

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER
58:EF:68:44:7C:4F	-55	100	623	179 2	8	54e	WPA2	CCMP

BSSID	STATION	PWR	Rate	Lost	Frames	Prob
58:EF:68:44:7C:4F	B4:9D:0B:5F:65:3C	-57	54e- 6	0	434	Red T
58:EF:68:44:7C:4F	A4:17:31:40:FB:46	-27	1e- 1e	0	39	

Figura 3-66 Captura handshake (elaboración propia)

El resultado de esta prueba de validación demuestra que los ataques de aircrack-ng sobre redes que aplican el estándar 802.11x no son posibles. Aircrack-ng no es capaz de descifrar la contraseña de usuario a través de diccionario.

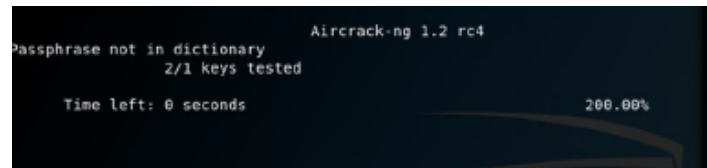


Figura 3-63 Proceso de rotura de contraseña (elaboración propia)

5 CONCLUSIONES Y LÍNEAS FUTURAS

En este capítulo se procede a exponer las conclusiones y líneas futuras detectadas tras la realización de este trabajo y que quieren servir como resumen y punto de partida para futuros trabajos relacionados con esta temática.

5.1 Conclusiones

El objetivo principal, tal y como establece el punto 1.2, de este trabajo era elaborar un documento técnico que permita a una organización bajo el paraguas del Esquema Nacional de Seguridad establecer un modelo de arquitectura de referencia para la implementación de un sistema de comunicaciones inalámbrico basado en el estándar general 802.11 WiFi seguro en un entorno corporativo seguro.

Respecto a la institución de estudio de este proyecto se ha elegido una institución del sector público debido a la amplia normativa en vigor que el CCN ofrece a través de las guías CCN-STIC. Relacionado con este aspecto la elección de un departamento universitario viene dada debido a que la guía CCN-STIC 803 “*Valoración de Sistemas en el ENS*”, Anexo I establece las medidas de seguridad necesarias para que un organismo como tal se adecúe a la normativa en vigor respecto a las medidas del Entorno Nacional de Seguridad. Respecto a este último punto el trabajo se ha basado en diferentes guías STIC que han aportado documentación para la realización del mismo.

Para la distribución de dichos puntos de acceso se realizó un mapa de calor en el cual se especificaban los materiales de construcción del área a abarcar y la posible atenuación que dichos materiales producían en la cobertura WiFi. Reduciendo la potencia de transmisión de los puntos de acceso para evitar una excesiva cobertura de radiación.

Posteriormente, se ha procedido con la complicada labor de configurar una red inalámbrica corporativa, complementada con una red de invitados. En dicha configuración se ha pretendido sintetizar y mostrar aquellos apartados que se han considerado más importantes.

Por último, se han realizado algunas pruebas pertinentes para comprobar y valorar que las medidas implementadas son efectivas, obviándose una serie de pruebas que darían un enfoque más amplio al proyecto.

5.2 Líneas futuras

Respecto a líneas futuras de trabajo relacionado con este proyecto se citan las siguientes:

- Implantar medidas de seguridad de mayor nivel, en este caso nivel ALTO. Sería incluso factible implantar medidas que incluyeran información clasificada.
- Realizar estudios para la ampliación de usuarios que permita un mayor aprovechamiento de los recursos disponibles, con la valoración de roles y privilegios de cada uno de ellos.
- La red propuesta no tiene utilidad si no es completada con una red cableada que le dé salida hacia recursos exteriores. Se plantea la posibilidad de acometer su aplicación hacia esta red cableada, así como sus repercusiones desde el punto de vista de la seguridad.
- Mejorar la defensa y su posterior valoración en ataques más específicos, tales como “*Denegación de Servicio*” (DoS), “*Hombre en Medio*” (MiTM). En la valoración del trabajo se ha incidido en la prueba de robo de credenciales, no se han acometido otros ataques de mucha actualidad.
- La seguridad implementada se basa en WPA2, el cercano despliegue de WPA3 puede suponer un nuevo campo de estudio.
- Abordar un proyecto que abarcase distintas disciplinas normativas en el ámbito de la seguridad, tales como la seguridad física, políticas, procedimientos, ciberseguridad, etc. Todas ellas son campos amplios, en constante cambio y con grandes posibilidades de desarrollo.

6 BIBLIOGRAFÍA

- [1] Fundamentos redes inalámbricas [en línea] Enlace: <https://www.redeweb.com/articulos/software/11-redes-inalambricas-fundamentales-para-internet-de-las-cosas/> [Último acceso: 05/01/2022]
- [2] ¿Qué es Zigbee? [en línea] Enlace: <https://zigbeealliance.org/es/solution/ZigBee/> [Último acceso: 05/01/2022]
- [3] ¿Qué es Bluetooth? Toda la información sobre el estándar inalámbrico [en línea] Enlace: <https://www.ionos.es/digitalguide/servidores/know-how/que-es-bluetooth/> [Último acceso: 05/01/2022]
- [4] Thread certified products [en línea] Enlace: <https://www.threadgroup.org/What-is-Thread/Thread-Benefits> [Último acceso: 05/01/2022]
- [5] NFC FORUM About the technology [en línea] Enlace: <https://nfc-forum.org/what-is-nfc/about-the-technology/> [Último acceso: 05/01/2022]
- [6] Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica [en línea] Enlace: <https://www.boe.es/buscar/act.php?id=BOE-A-2010-1330> [Último acceso: 05/01/2022]
- [6] Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010 [en línea] Enlace: <https://www.boe.es/buscar/doc.php?id=BOE-A-2015-11881> <https://www.boe.es/buscar/doc.php?id=BOE-A-2015-11881> [Último acceso: 05/01/2022]
- [7] Historia de las redes inalámbricas [en línea] Enlace: <https://histinf.blogs.upv.es/2010/12/02/historia-de-las-redes-inalambricas/> [Último acceso: 05/01/2022]
- [8] A. S. Tanenbaum y D. J. Wetherall, Redes de computadores, Editorial Pearson, 2012. ISBN 9780132126953
- [9] Wimax IEEE 802.16 [en línea] Enlace: http://www.oas.org/en/citel/infocitel/2009/septiembre/wimax_e.asp [Último acceso: 05/01/2022]
- [10] Tipos de redes de computadoras [en línea] Enlace: <https://www.todosobretusistemaoperativo.com/tipos-de-redes-de-computadoras/> [Último

acceso: 05/01/2022]

- [11] Tarjeta PCI Express Wireless N TP-LINK 300MPS [en línea] Enlace: <https://www.conectrolinformatica.com/tarjetas-wireless/5112-tarjeta-pci-express-wireless-n-tp-link-300mbps.html> [Último acceso: 05/01/2022]
- [12] Adaptador red inalámbrica [en línea] Enlace: <https://www.amazon.es/Startech-USB433ACD1X1-StarTech-com-Cable-Red/dp/B01N37NKBG> [Último acceso: 05/01/2022]
- [13] Transcend TS0MCF2PC Adaptador para Tarjetas de Memoria Compac Flash (PCMCIA) [en línea] Enlace: <https://www.amazon.es/Transcend-TS0MCF2PC-Adaptador-tarjetas-memoria/dp/B0009M069Y> [Último acceso: 05/01/2022]
- [14] Comunicaciones reunidas, puntos de acceso inalámbricos [en línea] Enlace: <https://www.crs1.es/gb/puntos-de-acceso-montaje-techo-serie-cap/4871-tp-link-eap115-punto-de-acceso-inalambrico-n-de-300-mbps-montaje-en-techo-portal-cautivo-2-antenas-internas.html> [Último acceso: 05/01/2022]
- [15] Linksys WRT54G [en línea] Enlace: <https://www.linksys.com/hn/support-article?articleNum=140196> [Último acceso: 05/01/2022]
- [16] Antenas WiFi [en línea] Enlace: https://www.amazon.es/s?k=ANTENAS+WIFI&__mk_es_ES=%C3%85M%C3%85%C5%BD%C3%95%C3%91&crd=3MM7EKE2FZP2N&srefix=antenas+wifi%2Caps%2C236&ref=nb_sb_noss_1 [Último acceso: 05/01/2022]
- [17] Institute of Electrical and Electronics Engineers [en línea] Enlace: <https://www.ieee.org/> [Último acceso: 05/01/2022]
- [18] Real Academia de la Lengua Española [en línea] Enlace: <https://dle.rae.es/est%C3%A1ndar> [Último acceso: 05/01/2022]
- [19] El nuevo estándar 802.11AX [en línea] Enlace: <https://tecnocompras6.webnode.com.co/news/el-nuevo-estandar-802-11ax-alcanza-una-velocidad-maxima-de-10-gbps/> [Último acceso: 05/01/2022]
- [20] Caos en la seguridad WiFi [en línea] Enlace: <https://www.xataka.com/seguridad/caos-en-la-seguridad-wifi-un-repaso-a-las-vulnerabilidades-de-wep-wap-y-wap2> [Último acceso: 05/01/2022]
- [21] Albert Gonzalez [en línea] Enlace: <https://www.elhacker.net/hackers-famosos-albert-gonzalez.html> [Último acceso: 05/01/2022]
- [22] Aircrack-ng [en línea] Enlace: <http://aircrack-ng.org/doku.php?id=es:tkiptun-ng> [Último acceso: 05/01/2022]
- [23] CCN-CERT Vulnerabilidades WPA-TKIP [en línea] Enlace: <https://www.ccn-cert.cni.es/gl/seguridade-ao-dia/noticias-de-actualidade/744-vulnerabilidad-en-wpa-con-tkip.html> [Último acceso: 05/01/2022]
- [24] SpeedCheck Acceso protegido WPA2 [en línea] Enlace: <https://www.speedcheck.org/es/wiki/wpa2/> [Último acceso: 05/01/2022]
- [25] CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) [en línea] Enlace:

- [https://www.cybertraining365.com/cybertraining/Topics/CCMP_\(Counter_Mode_with_Cipher_Block_Chaining_Message_Authentication_Code_Protocol\)](https://www.cybertraining365.com/cybertraining/Topics/CCMP_(Counter_Mode_with_Cipher_Block_Chaining_Message_Authentication_Code_Protocol)) [Último acceso: 05/01/2022]
- [26] WPA2-Hole196 [en línea] Enlace: <https://blog.segu-info.com.ar/2010/08/wpa2-hole196-faq-sobre-la-explotacion.html> [Último acceso: 05/01/2022]
- [27] ¿Qué es WPA2? [en línea] Enlace: <https://www.netspotapp.com/es/what-is-wpa3.html> [Último acceso: 05/01/2022]
- [28] The Galois/Counter Mode of Operation (GCM) [en línea] Enlace: <https://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/gcm/gcm-spec.pdf> [Último acceso: 05/01/2022]
- [29] Las diferencias entre WPA-Personal y WPA-Enterprise [en línea] Enlace: <https://www.tp-link.com/ar/support/faq/500/> [Último acceso: 05/01/2022]
- [30] Máster DIRETIC TEL_4 Sesión 7 Seguridad en Redes Inalámbricas. Profesor don Carlos Zamorano Pinal
- [31] INCIBE Seguridad Redes WiFi [en línea] Enlace: <https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia-de-seguridad-en-redes-wifi.pdf> [Último acceso: 05/01/2022]
- [32] 802.11 State Machine [en línea] Enlace: <https://notasinalambricas.wordpress.com/tag/802-11-state-machine/> [Último acceso: 05/01/2022]
- [33] Notas inalámbricas [en línea] Enlace: <https://notasinalambricas.wordpress.com/tag/associated/> [Último acceso: 05/01/2022]
- [34] CCN-CERT_BP_11_Recomendaciones redes WIFI [en línea] Enlace: <https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/3143-ccn-cert-bp-11-recomendaciones-redes-wifi-corporativas-1/file.html> [Último acceso: 05/01/2022]
- [35] Seguridad redes WiFi: aproximación para el empresario [en línea] Enlace: <https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia-de-seguridad-en-redes-wifi.pdf> [Último acceso: 05/01/2022]
- [36] Guía CCN-STIC_001 Información Clasificada en la Administración [en línea] Enlace: <https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/1579-ccn-stic-001-informacion-clasificada-en-la-administracion.html> [Último acceso: 05/01/2022]
- [37] Ataques en redes LAN [en línea] Enlace: <https://www.redusers.com/noticias/ataques-en-redes-lan-que-es-y-como-functiona-el-sniffing/> [Último acceso: 05/01/2022]
- [38] MAC Spoofing: qué es y cuándo se utiliza [en línea] Enlace: <https://www.ionos.es/digitalguide/servidores/know-how/que-es-el-mac-spoofing/> [Último acceso: 05/01/2022]
- [39] Aircrack-ng Ataque de punto de acceso falso [en línea] Enlace: <https://fwhibbit.es/aircrack-ng-iv-ataque-de-punto-de-acceso-falso> [Último acceso: 05/01/2022]
- [40] ¿Qué es un ataque Man-in-the-Middle? [en línea] Enlace: <https://www.kaspersky.es/blog/que-es-un-ataque-man-in-the-middle/648/> [Último acceso: 05/01/2022]
- [41] ¿Qué son los ataques DoS y DDoS? [en línea] Enlace: <https://www.osi.es/es/actualidad/blog/2018/08/21/que-son-los-ataques-dos-y-ddos> [Último

acceso: 05/01/2022]

- [42] INCIBE Seguridad Redes WiFi [en línea] Enlace: <https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia-de-seguridad-en-redes-wifi.pdf> [Último acceso: 05/01/2022]
- [43] Redes Zone, filtrado MAC [en línea] Enlace: <https://www.redeszone.net/2018/05/05/filtrado-mac-router/> [Último acceso: 05/01/2022]
- [44] Centro Criptologico Nacional [en línea] Enlace: <https://www.ccn-cert.cni.es/> [Último acceso: 05/01/2022]
- [45] Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica [en línea] Enlace: <https://www.boe.es/buscar/act.php?id=BOE-A-2010-1330> [Último acceso: 05/01/2022]
- [46] Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica [en línea] Enlace: <https://www.boe.es/buscar/doc.php?id=BOE-A-2015-11881> [Último acceso: 05/01/2022]
- [47] Guía CCN-STIC-804 Medidas de implantación del ENS [en línea] Enlace: <https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/505-ccn-stic-804-medidas-de-implantacion-del-ens/file.html> [Último acceso: 05/01/2022]
- [48] Ventajas y desventajas del software libre [en línea] Enlace: <https://empresas.blogthinkbig.com/ventajas-y-desventajas-del-software-libre/> [Último acceso: 05/01/2022]
- [49] Ventajas y desventajas del software libre [en línea] Enlace: <http://andreitamedina.blogspot.com/2012/04/ventajas-y-desventajas-del-software.html> [Último acceso el 05 de enero de 2022]
- [50] D-link software gratuito de gestion de redes WiFi [en línea] Enlace: https://eu.dlink.com/es/es/press-centre/press-releases/2015/june/16/es_d-link-lanza-el-software-gratuito-cwm [Último acceso: 05/01/2022]
- [51] DD-WRT Firmware [en línea] Enlace: <https://www.redeszone.net/tutoriales/configuracion-routers/que-es-dd-wrt-instalar-router/> <https://dd-wrt.com> [Último acceso: 05/01/2022]
- [52] What is Tomato? [en línea] Enlace: <https://advancedtomato.com> [Último acceso: 05/01/2022]
- [53] OpenWRT [en línea] Enlace: <https://openwrt.org> [Último acceso: 05/01/2022]
- [54] Metageek Software [en línea] Enlace: <https://www.metageek.com> [Último acceso: 05/01/2022]
- [55] Network Performance Monitor [en línea] Enlace: <https://www.solarwinds.com/es/network-performance-monitor/use-cases/wifi-monitor> [Último acceso: 05/01/2022]
- [56] Netspotapp, WiFi manager [en línea] Enlace: <https://www.netspotapp.com> [Último acceso: 05/01/2022]
- [57] Las mejores herramientas para hacking etico y seguridad WiFi [en línea] Enlace: <https://www.softzone.es/programas/utilidades/mejores-herramientas-hacking-etico-wi-fi/> [Último acceso: 05/01/2022]
- [58] Universidad de Extremadura, Vicerrectorado de Planificación Académica [en línea] Enlace: https://www.unex.es/organizacion/gobierno/vicerrectorados/vicecoor/index__html

[Último acceso: 05/01/2022]

- [59] Guía CCN-STIC_816 Seguridad en Redes Inalámbricas [en línea] Enlace: <https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2317-ccn-stic-816-seguridad-en-redes-inalambricas-en-el-ens/file.html> [Último acceso: 05/01/2022]
- [60] Guía CCN-STIC-803 Valoración de los sistemas [en línea] Enlace: <https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/2509-ccn-stic-803-valoracion-de-sistemas-en-el-ens-anexo-i-universidades/file.html> [Último acceso: 05/01/2022]
- [61] Guía CCN-STIC-803 Valoración de los sistemas Anexo I [en línea] Enlace: <https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/2509-ccn-stic-803-valoracion-de-sistemas-en-el-ens-anexo-i-universidades/file.html> [Último acceso: 05/01/2022]
- [62] ISO/IEC 27002:2013 [en línea] Enlace: <https://normaiso27001.es> [Último acceso: 05/01/2022]
- [63] Guía CCN-STIC-801 ENS Responsabilidades y funciones [en línea] Enlace: <https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/501-ccn-stic-801-responsabilidades-y-funciones-en-el-ens/file.html> [Último acceso: 05/01/2022]
- [64] ISO/IEC 27000 [en línea] Enlace: https://ingertec.com/iso-27001/?gclid=Cj0KCQiAoNWOBhCwARIsAAiHnEiuvDJ6HAb3kXISZX7Y8swfSKmWhwnd7OkQ3AoFZND0idxd4DxuZ7caArMTEALw_wcB [Último acceso: 05/01/2022]
- [65] ISO/IEC 27002:2013 [en línea] Enlace: <https://ostec.blog/es/generico/iso-27002-buenas-practicas-gsi/> <https://ostec.blog/es/generico/iso-27002-buenas-practicas-gsi/> [Último acceso: 05/01/2022]
- [66] SANS CIS Critical Security Controls [en línea] Enlace: <https://blog.netwrix.com/2018/02/01/top-20-critical-security-controls-for-effective-cyber-defense/> [Último acceso: 05/01/2022]
- [67] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales [en línea] Enlace: <https://www.boe.es/doue/2016/119/L00001-00088.pdf> [Último acceso: 05/01/2022]
- [68] Master DIRETIC TEL2 Sesión 4 Redes de banda ancha, profesores: Felipe Gil Castiñeira y Pablo Fondo Ferrerio
- [69] Guía CCN-STIC-105 Catalogo Productos STIC [en línea] Enlace: <https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2536-ccn-stic-105-catalogo-de-productos-de-seguridad-de-las-tecnologias-de-la-informacion-y-la-comunicacion/file.html> [Último acceso: 05/01/2022]
- [70] Punto de acceso Ruckus R610 [en línea] Enlace: <https://docs.ruckuswireless.com/unleashed/200.1.9.12/c-OverviewSetupProcess.html> [Último acceso: 05/01/2022]
- [71] Hoja datos punto de acceso Ruckus R610 [en línea] Enlace: <https://es.commscope.com/globalassets/digizuite/506635-ds-ruckus-R610-es.pdf> [Último acceso: 05/01/2022]

- [72] Panel frontal Ruckus R610 [en línea] Enlace: <https://docs.ruckuswireless.com/unleashed/200.4/c-R610.html> [Último acceso: 05/01/2022]
- [73] Ubicación geografica de las instalaciones [en línea] Enlace: <https://www.google.es/maps/@40.4010803,-3.8091817,68m/data=!3m1!1e3?hl=es> [Último acceso: 05/01/2022]
- [74] Basic TACACS Configuration Example [en línea] Enlace: <https://www.cisco.com/c/en/us/support/docs/security-vpn/terminal-access-controller-access-control-system-tacacs-/10368-basictacacs.html> [Último acceso: 05/01/2022]
- [75] Access control protocol TACACS [en línea] Enlace: <https://www.rfc-editor.org/rfc/pdf/rfc1492.txt.pdf> [Último acceso: 05/01/2022]
- [76] Mapas de calor, Acrylic [en línea] Enlace: <https://www.acrylicwifi.com/programas-software-herramientas-wifi/análisis-cobertura-wifi-acrylic-heatmaps-mapas-de-cobertura/> [Último acceso: 05/01/2022]
- [77] Analisis del espectro WiFi [en línea] Enlace: <https://www.acrylicwifi.com/programas-software-herramientas-wifi/escaner-wifi-acrylic-wifi-gratuito/> [Último acceso: 05/01/2022]
- [78] Factores que influyen en una red WiFi [en línea] Enlace: <https://www.netspotapp.com/es/wifi-signal-strength-and-its-impact.html> [Último acceso: 05/01/2022]
- [79] ¿Qué es WDS? [en línea] Enlace: <https://www.redeszone.net/2018/04/01/wds-mejorar-cobertura-wi-fi/> [Último acceso: 05/01/2022]
- [80] Sistemas WiFi Mesh o de malla [en línea] Enlace: <https://www.xatakamovil.com/conectividad/sistemas-wifi-mesh-malla-que-que-ventajas-desventajas-tienen-modelos-recomendados> [Último acceso: 05/01/2022]
- [81] Interconexión Ethernet [en línea] Enlace: <https://www.redeszone.net/reportajes/listas/mejores-wi-fi-mesh-interconexion-ethernet/> [Último acceso: 05/01/2022]
- [82] Jitter [en línea] Enlace: <https://www.speedcheck.org/es/wiki/jitter/> [Último acceso: 05/01/2022]
- [83] ISO/IEC 27002:2013 Control de accesos [en línea] Enlace: <https://normaiso27001.es/a9-control-de-acceso/> [Último acceso: 05/01/2022]
- [84] FreeRadius: WiFi mas seguro [en línea] Enlace: <https://www.masquetcas.com/tutorial/wifi-mas-seguro-con-freeradius/> [Último acceso: 05/01/2022]
- [85] MySQL Enterprise monitor [en línea] Enlace: <https://www.mysql.com/products/enterprise/monitor.html> [Último acceso: 05/01/2022]
- [86] Guía CCN-STIC-816 Seguridad en Redes Inalámbricas [en línea] Enlace: <https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2317-ccn-stic-816-seguridad-en-redes-inalambricas-en-el-ens/file.html> [Último acceso: 05/01/2022]
- [87] Insiders [en línea] Enlace: <https://intelsynet.com/es/que-es-un-insider-en-la-empresa/> [Último acceso: 05/01/2022]
- [88] ¿Que son y para que sirven los SIEM, IDS e IPS? [en línea] Enlace: <https://www.incibe.es/protege-tu-empresa/blog/son-y-sirven-los-siem-ids-e-ips> [Último

acceso: 05/01/2022]

- [89] Kismet, wireless network and device detector [en línea] Enlace: <https://www.kismetwireless.net/> [Último acceso: 05/01/2022]
- [90] Kismet IU [en línea] Enlace: https://www.kismetwireless.net/development/kismet_webui_tour/ [Último acceso: 05/01/2022]
- [91] Bandas RF: ISM-ICM [en línea] Enlace: https://dmd2.es/banda_ism_icm/ [Último acceso: 05/01/2022]
- [92] <https://securityhacklabs.net/articulo/usando-kismet-para-ver-la-actividad-de-un-usuario-de-wi-fi-a-traves-de-las-paredes> [Último acceso: 05/01/2022]
- [93] Guia CCN-STIC-201 Organización y gestión para la seguridad TIC [en línea] Enlace: <https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/45-ccn-stic-201-estructura-de-seguridad/file.html> [Último acceso: 05/01/2022]
- [94] CCN-STIC-406 Seguridad en redes inalámbricas [en línea] Enlace: <https://www.ccn-cert.cni.es/abrir-sesion.html> [Último acceso: 05/01/2022]