Seguridad en redes wifi:

una guía de aproximación para el empresario

GOBIERNO DE ESPAÑA
MINISTERIO DE ECONOMÍA Y EMPRESA

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

protege tu empresa

ÍNDICE

ÍNDICE

1 INTRODUCCIÓN

Hasta hace pocos años, la idea de interconectar dispositivos tecnológicos estaba ligada a la clásica distribución de una red de ordenadores cableada que nos permitía por un lado, tener acceso a un servidor, normalmente de datos y por otro, a Internet. No era de extrañar, encontrarse en muchas compañías mesas de trabajo con un cable de red como único utensilio visible, de tal manera que cualquiera con un portátil pudiera conectarse para poder así realizar su trabajo.

Hoy en día, esta concepción ha cambiado radicalmente. El uso de la tecnología inalámbrica se ha extendido de tal manera que nadie concibe un sistema en el que para conectarse, sea necesario hacer uso de cables.

Nos hallamos inmersos en una era inalámbrica en la que dispositivos como ordenadores personales, *smartphones* o *tablets* y elementos IoT[1] pueden llegar a estar interconectados entre sí sin necesidad de hacer uso del cable, a través de ondas electromagnéticas, incorporando esta capacidad de forma nativa, sin necesidad de añadirla artificialmente.

La aparición de la red inalámbrica se entiende como una **extensión** de una red de ordenadores interconectados físicamente, por cable, con un único objetivo: proporcionar libertad de movimientos evitando tener que situarse en una ubicación física determinada a la hora de conectarse a los recursos que pueda ofrecer una organización.

Pero a pesar de las ventajas que pueda ofrecer esta funcionalidad, no está exenta de riesgos asociados a su uso, que se deberán analizar y tener en cuenta en cualquier empresa a la hora de configurar políticas y medidas que los mitiguen o minimicen y que a su vez, garanticen la seguridad de las comunicaciones **[Ref - 1].**

En esta guía se explican:

- **Los conceptos básicos sobre tecnologías wifi.**
- **Características y riesgos.**
- **Configuración de las WLAN.**
- **La configuración del router.**
- **Medidas de seguridad básicas y avanzadas**

Contar con una configuración segura de tu red inalámbrica será de vital importancia a la hora de preservar la privacidad e integridad de las comunicaciones y en última

1. El Internet de las Cosas (en inglés *Internet of Things*, abreviado IoT), es una red de objetos cotidianos interconectados con acceso a Internet.

1

instancia, de la información que por ésta discurra. En esta línea, este documento proporcionará una guía básica de buenas prácticas que tiene como objetivo ayudar a cualquier tipo de organización, a comprender y mejorar la seguridad de sus redes inalámbricas, indistintamente de su dimensión para que puedan proteger su principal activo, la información.

Son muchas las tecnologías inalámbricas que se vienen desarrollando en los últimos años y es lógico pensar que seguirán desarrollándose. Por lo tanto, estas buenas prácticas quedarán supeditadas a una continua revisión directamente relacionada con el propio avance tecnológico, a la aparición constante de vulnerabilidades o a la aprobación de nuevos estándares como el recientemente aparecido WPA3.

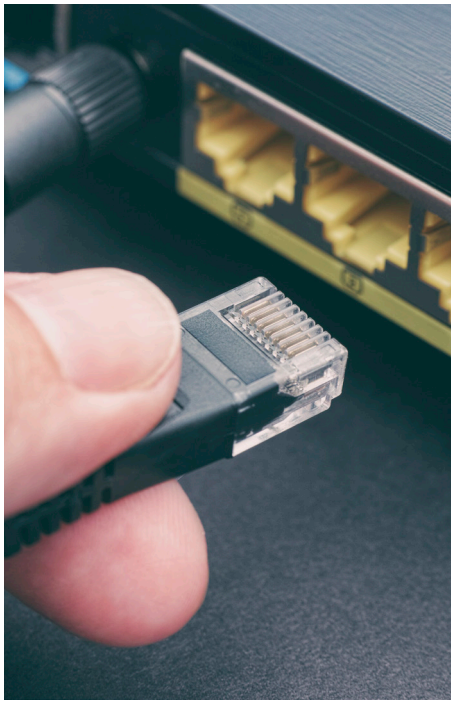
2 LAS REDES INALÁMBRICAS

2.1. Definición

Definiremos red inalámbrica, como aquella formada por dispositivos capaces de intercomunicarse entre sí o con otra red (como Internet), sin necesidad de elementos físicos que las conecten como pueden ser los cables.

Teniendo en cuenta que existen muchos tipos de redes inalámbricas cuya diferencia radica en aspectos como la arquitectura, tecnología o estándares de comunicación entre otros, en esta guía nos centraremos en las más extendidas, las Redes de Área Local Inalámbricas, conocidas como WLAN (en inglés, *Wireless Local Area Networks*) o redes wifi.

"Una **red inalámbrica** es aquella formada por dispositivos capaces de intercomunicarse entre sí o con otra red, sin necesidad de elementos físicos que las conecten [...]"



2.1.1 Introducción al wifi

Wifi (sustantivo común en español, incluido en el diccionario de la RAE y proveniente de la marca Wi-Fi), es un sistema que permite la interconexión inalámbrica, dentro de un área determinada, de dispositivos electrónicos, cuyo uso más común y extendido es el acceso a Internet.

Wi-Fi es una marca de la Wi-Fi Alliances (Alianza Wi-Fi en español). Se trata de una organización sin ánimo de lucro que promueve y certifica la tecnología y productos wifi, comprobando que se ajustan a los estándares de interconectividad compatibles con IEEE 802.11 (especifica las normas de funcionamiento de una red de área local inalámbrica), si bien los costes asociados a esta certificación hacen que no todos los productos se sometan a este proceso. La falta del logotipo Wi-Fi no implica que un dispositivo sea incompatible con cualquier otro dispositivo wifi certificado.

2

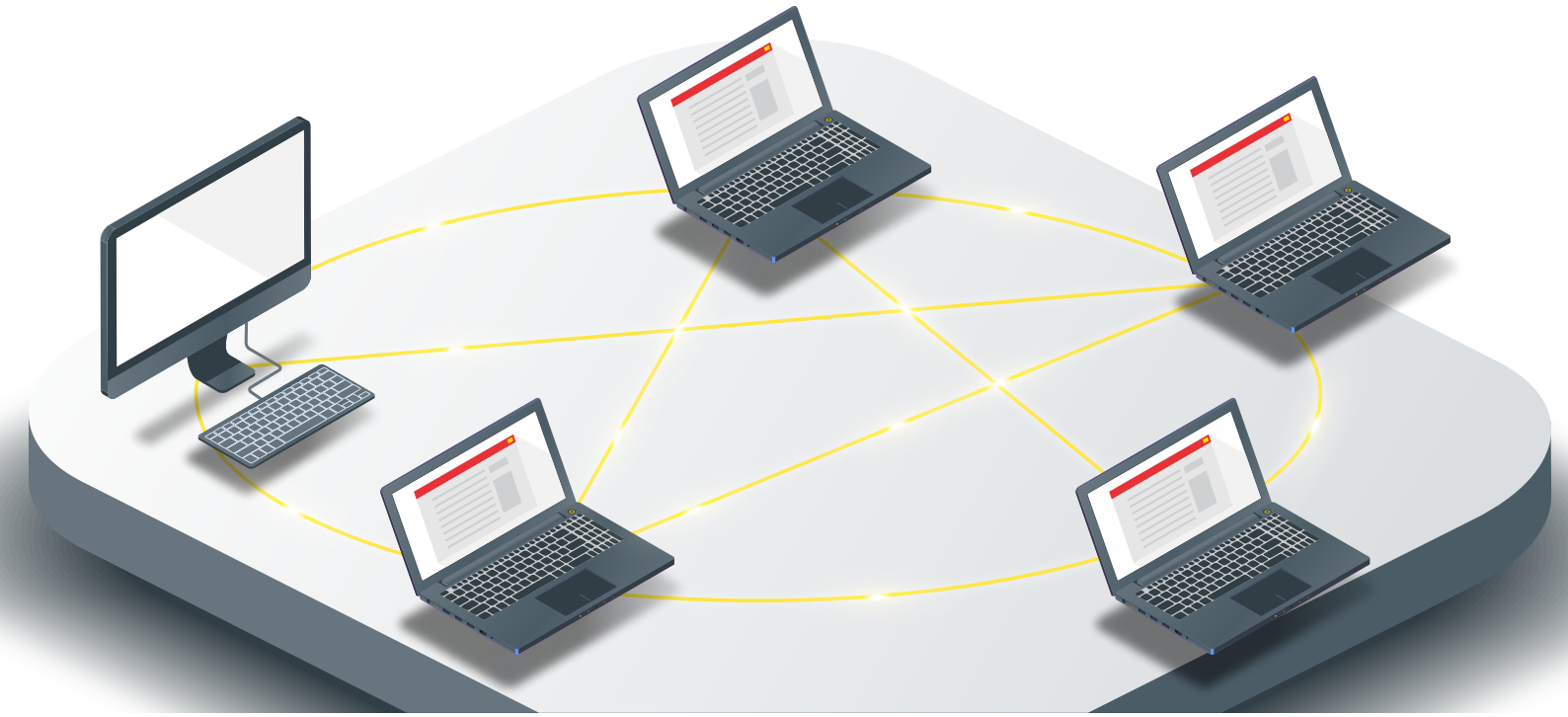
2.2. Componentes

- **Dispositivos cliente:** son los que solicitan la conexión a la red inalámbrica como los ordenadores portátiles, *tablets, smartphones*, etc.
- **Punto de acceso** (en inglés *Access Point*): elemento tecnológico que conecta los dispositivos clientes entre sí o con el resto de la infraestructura cableada de la organización. También sirven como puertas de enlace a otras redes, como Internet. Comúnmente se le conoce como *router*, aunque este dispositivo también es capaz de realizar otras tareas.

2.3. Tipos

Se trata de la forma en la que estará configurada la red a la hora de intercambiar los datos que por ella transcurran. Desde el punto de vista de los dispositivos que se conectan a ella, dentro de una red inalámbrica habrá dos tipos:

- **Modo Ad Hoc**, donde no existen puntos de acceso o *routers* y los dispositivos cliente se comunican entre sí directamente. Por ejemplo, a través de tecnologías como *Bluetooth*[2] o *WI-FI Direct* [3].

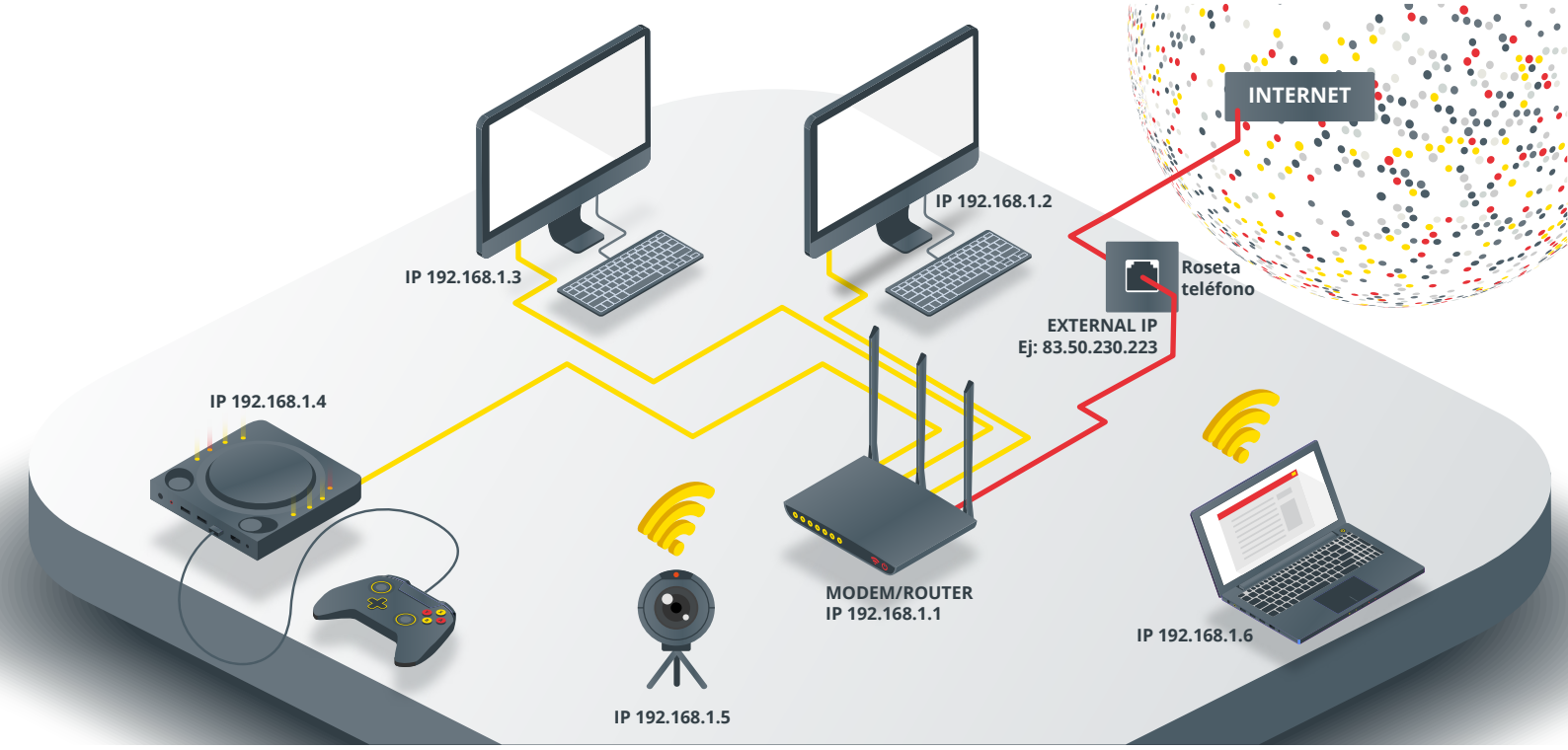


2. *Bluetooth* es una tecnología inalámbrica de radio de corto alcance, cuyo objetivo es eliminar los cables en las conexiones entre dispositivos electrónicos, simplificando así las comunicaciones entre teléfonos móviles, ordenadores, cámaras digitales y otros dispositivos informáticos operando bajo la banda de radio de 2.4 GHz de frecuencia.

3. *WiFi Direct* está definido por la Wi-Fi Alliance como una certificación para dispositivos que soportan una tecnología que permite la comunicación directa, sin unirse a una red tradicional o punto de acceso.

2

» **Modo infraestructura:** aquí es necesario el uso de los puntos de acceso o *routers* para la interconexión de dispositivos. Este tipo de red es la que comúnmente se utiliza en empresas y hogares. Por medio de un punto de acceso o del *router*, se accede a los distintos recursos de red, como pueden ser otros dispositivos, servidores, impresoras, etc.



2.4. Ventajas y desventajas

Como hemos evidenciado, la principal ventaja de contar con un mecanismo de red inalámbrico es la **ausencia de cables** y por lo tanto, la ausencia de preocupaciones por el estado, mantenimiento y organización de los mismos.

Fruto de esta ausencia de cables es el alto grado de movilidad, siendo esta una de las mayores ventajas que otorga esta tecnología. De esta manera, se evitan las limitaciones de ubicación que supone una instalación cableada donde únicamente se tiene acceso a la red en aquellos puntos donde el cable esté a disposición del usuario.

Uno de los principales inconvenientes asociados a este tipo de conectividad es la naturaleza abierta y accesible de la misma, lo que la convierte en una tecnología más vulnerable que el cable. Además, debido a interferencias de señal y otros

2

factores como por ejemplo, los ambientales, podría verse afectada la velocidad de navegación o incluso la propia disponibilidad de la señal.

En resumen, la tecnología wifi permite dar servicio a varios usuarios que podrán conectarse cuando así lo deseen y en cualquier lugar donde llegue la señal, mientras que con el cable solo podrá conectarse aquel que haga uso de dicho cable en el puesto habilitado.

2.5. Riesgos de redes inalámbricas

"Al tratarse de una tecnología inalámbrica, cualquiera que se encuentre dentro de su rango de acción podría llevar a cabo acciones maliciosas."

A los riesgos y amenazas propios de redes cableadas hay que añadir los inherentes a las redes wifi. Al tratarse de una tecnología inalámbrica, cualquiera que se encuentre dentro de su rango de acción podría llevar a cabo acciones maliciosas. Así pues, nos podremos encontrar los siguientes tipos de amenazas:

- **Denegación de servicio (DoS) [Ref - 2]:** se trata de incapacitar la infraestructura inalámbrica a través de peticiones de servicio masivas a los puntos de acceso, provocando que los sistemas se vean incapaces de atender a tantas peticiones. Mediante este ataque se busca sobrecargar el punto de acceso o el *router* e impedir que los usuarios legítimos hagan uso de los servicios que este presta.
- ***Man-in-the-middle:*** se basa en que el atacante pueda situarse entre el emisor y el receptor, suplantando una de las partes y haciendo creer a la otra que está hablando con el legítimo destinatario de la comunicación, o incluso suplantando al punto de acceso (*Rogue Access Point* [4]).
- **Ataques por fuerza bruta [Ref - 3]:** método consistente en hacer uso de todas las contraseñas posibles cuya finalidad es averiguar las claves criptográficas de la comunicación o de las que dan acceso a la red wifi. A pesar

4. Es un punto de acceso inalámbrico que se ha instalado en una red segura sin la autorización explícita de un administrador de red local, bien porque lo haya agregado un empleado con buenas intenciones o un atacante malintencionado.

2

de que parezca poco probable conseguirlas, en Internet existen multitud de herramientas gratuitas que permiten hacerse con las claves de redes que no cuenten con algoritmos criptográficos o claves robustas **[Ref - 4]**.

- ***Eavesdropping:*** captura de tráfico de red no autorizado realizado a través de alguna herramienta como antenas de gran alcance. El objetivo es capturar la información que transmitimos, que podría ser completa si no se encuentra cifrada o, en caso contrario, hacerse con patrones de comportamiento para intentar un descifrado.
- ***MAC Spoofing:*** se trata de suplantar la dirección MAC[5] de un dispositivo permitido cuando el punto de acceso tenga configurada una lista de este tipo de direcciones permitidas.

5. De sus siglas en inglés *Media Access Control*, la dirección MAC es un identificador único e irrepetible que identifica todo dispositivo conectado a una red. También es conocida como dirección física.

3 CONFIGURACIÓN DE SEGURIDAD EN REDES WLAN

"Es muy importante contar con las medidas de seguridad y protección necesarias [...]"

Dentro del marco organizativo de una empresa es necesario que exista una configuración de seguridad establecida y documentada que garantice la seguridad necesaria para preservar la privacidad de la información. Para alcanzar este nivel de seguridad, se deberán incluir medidas como las que se describen a continuación.

3.1 Reflejar cuál será la arquitectura de seguridad

Se trata de una cuestión documental donde se especificará cómo está diseñada la red inalámbrica y cuál será su sistema de gestión, reflejando aspectos como los siguientes:

- Cuál será la cobertura de los puntos de acceso. Esta medida será tomada en consideración antes de la ubicación física de los mismos. El objetivo es minimizar la cantidad de señal fuera del perímetro controlado por la organización.
- En el ámbito empresarial, la red inalámbrica deberá ser modo infraestructura. Esto quedará reflejado en la arquitectura de seguridad. Por lo tanto, se utilizarán puntos de acceso u otros dispositivos de interconexión (*routers*), tanto para conectar los dispositivos que se quieran conectar a la red inalámbrica, como para conectar otros puntos de acceso entre sí.

3.2 Autenticación

Se trata de un proceso que deberá tener en cuenta los siguientes aspectos:

- Establecer cuál será el tipo de autenticación de la red

3

inalámbrica. Este se podrá realizar a través de claves precompartidas o a través de mecanismos de autenticación mutua.

El método de claves precompartidas (PSK), basa su funcionalidad en la existencia de una única clave de conexión a la red inalámbrica compartida por todos los equipos y usuarios.

En cambio, la autenticación mutua, es un método más seguro que permite un proceso de autenticación en el que cada cliente dispondrá de sus propias credenciales de acceso. Sin embargo, este método requerirá de infraestructura basada en un servidor de autenticación.

- Los mecanismos de autenticación serán los empleados para la autenticación, tanto del servidor como del cliente (en el caso de utilizar autenticación mutua).
- Por norma general, el servidor se autentica frente al cliente a través de un certificado, mientras que para la autenticación del cliente se utilizan mecanismos de un solo factor, como contraseñas, *tokens*, etc. En el caso de utilizar contraseñas, estas deberán ser lo más robustas posibles, por lo que deberá aplicarse una **política de contraseñas [Ref - 5],** que indiquen tanto los requisitos que estas deben cumplir (como que sean de al menos 8 dígitos que combinen minúsculas, mayúsculas, números y caracteres especiales), tiempo de renovación, intentos máximos permitidos, etc.
- En caso de considerarse necesario, se puede hacer uso de la autenticación de doble factor **[Ref - 6].**
- El protocolo encargado del transporte deberá estar encapsulado, lo que aumentará la seguridad del proceso de autenticación.

Es muy importante contar con las medidas de seguridad y protección necesarias, ya que en caso de verse comprometido, un atacante podría acceder a la red, y por lo tanto a la información, sin necesidad de utilizar una conexión física.

3.3. Distinción entre dispositivos corporativos y clientes externos

Para llevar a cabo una correcta configuración de seguridad en redes inalámbricas en el ámbito empresarial, será necesario distinguir entre los equipos que serán considerados como corporativos y equipos de personal externo.

Los equipos corporativos serán los que se encuentren bajo el control de la organización y de sus políticas de seguridad.

Al contrario que estos, los equipos externos no se someterán al control de la organización, ni estarán sujetos a ninguna política de seguridad interna. Eso sí, deberán contar con una alta restricción en cuanto a permisos de acceso, de tal

3

"Cuando hablamos de seguridad en redes inalámbricas, la monitorización de la seguridad es un aspecto prioritario [...]"

forma que únicamente puedan acceder a los recursos que sean abiertos y de acceso público.

Además, dentro de las políticas de seguridad con las que debe contar cualquier organización, deberá existir una específica donde queden reflejadas las medidas de protección y seguridad con las que deberá contar la red inalámbrica, estableciendo qué requisitos deberán cumplir, tanto los equipos corporativos (actualización de antivirus, parches del sistema operativo, política de actualizaciones de software **[Ref - 7]**, cortafuegos, etc.), como los dispositivos externos, que quieran conectarse a la misma.

Por lo que, habrá que tener en cuenta aspectos como los siguientes:

- Para que cada dispositivo cliente únicamente acceda solo a los recursos que le sean necesarios, se deberá controlar el acceso a la red.
- Como norma general, solo deberán estar habilitados aquellos recursos o servicios de red que sean necesarios. El resto es recomendable deshabilitarlos por defecto.
- Mucho cuidado con las conexiones duales. Se trata de conexiones que permiten la conexión simultánea del dispositivo cliente a dos o más redes, como podría ser una inalámbrica y otra física cableada. Un atacante podría conectarse a la red inalámbrica y lanzar un ataque sobre la red física, lo que pondría en riesgo la integridad de la información. Para evitarlo, será necesario establecer una política clara sobre el uso de este tipo de redes, indicando cuáles están autorizadas, cuáles prohibidas y bajo qué circunstancias, aunque lo más recomendable es que por defecto no se permitan.

3.4. Configuración estandarizada

Es muy recomendable que la configuración de seguridad de la infraestructura inalámbrica de la organización, se pueda desplegar automáticamente en todos los dispositivos. De esta forma, se establece una línea base de seguridad que homogeniza los componentes inalámbricos de la organización, aportando consistencia y uniformidad, reduciendo el tiempo

3

a la hora de desplegar la configuración en los dispositivos, lo que permitirá detectar y corregir cambios no autorizados en la misma.

3.5. Registrar la actividad de los usuarios

Es necesario registrar la actividad tanto de los usuarios como de los administradores, sobre todo si estos, realizan modificaciones en la configuración de seguridad. Además, es muy importante llevar un registro detallado de los intentos de conexión a la red inalámbrica, con independencia de que hayan sido exitosos o fallidos.

3.6. Monitorización

Cuando hablamos de seguridad en redes inalámbricas, la monitorización de la seguridad es un aspecto prioritario, ya que permite conocer el estado de seguridad de la red, identificando y en su caso, reaccionando con la mayor celeridad posible ante ataques, fallos de seguridad o cualquier otro tipo de problema, atendiendo especialmente a dos aspectos:

- **Monitorización de posibles** ataques, donde un individuo no autorizado alterara o interrumpiera las comunicaciones inalámbricas.
- **Monitorización de vulnerabilidades**, que se llevarán a cabo sobre los distintos componentes que conforman la infraestructura inalámbrica. Las acciones serán, en primer lugar, identificar las posibles vulnerabilidades para a continuación aplicar los parches de seguridad. Por último es recomendable verificar las configuraciones de seguridad establecidas y modificarlas cuando sea necesario.

3.7. Auditorías de seguridad

Una organización con sistemas e infraestructuras tecnológicas deberá contar con una serie de auditorías de seguridad **[Ref - 8]** en sus diferentes ámbitos que deberán realizarse periódicamente. Las redes inalámbricas no serán ajenas a estas auditorías, ya que son la mejor forma de verificar que la red cumple con las políticas de seguridad establecidas en la organización. Para llevarlas a la práctica se pueden hacer uso de los análisis de vulnerabilidades y de la configuración de los puntos de acceso o de los análisis de incidentes y de la aplicación de las medidas correctoras o mitigadoras sobre los mismos.

4 EL *ROUTER* Y LAS MEDIDAS DE SEGURIDAD

El *router* es el dispositivo que actúa como punto de acceso entre los dispositivos inalámbricos de la organización o de una red privada. Además, en muchos casos, sirve como puerta de enlace entre ésta e Internet. Mantener este dispositivo correctamente configurado será de gran importancia para la mantener la seguridad de la organización.

4.1. Riesgos de un *router* mal configurado

Cuando un *router* no cuenta con las medidas de seguridad y las configuraciones apropiadas podemos sufrir las siguientes consecuencias:

- **Robo de información confidencial.** Cuando un intruso se conecta a nuestra red privada podría llegar a acceder a nuestra información y si cuenta con los suficientes conocimientos podría acceder a los dispositivos de la empresa, así como a los datos que estamos enviando y recibiendo de Internet.
- **Utilizar la red para realizar acciones ilegales.** Si un delincuente logra acceder a nuestro *router*, podrá usar los dispositivos que hay en nuestra red para llevar a cabo acciones ilegales o maliciosas, como conectarse de manera repetitiva a una página web para sobrecargarla e impedir que funcione de manera correcta como el que hace poco sufrieron compañías como Twitter, Spotify o Ebay **[Ref - 9]**.
- **Vinculación con lo que ocurra en tu red.** Cuando contratamos una conexión a Internet, nuestro proveedor vincula la dirección IP que tengamos en ese momento con el nombre del titular, de la misma manera que un número de teléfono está asociado a su suscriptor. Cualquier acción, ilegal o no, que se lleve a cabo desde nuestra red estará asociada directamente con el titular de la línea, es decir, con nosotros, y aunque se demuestre que hubo alguna intrusión en nuestro sistema, puede generarnos algún quebradero de cabeza.
- **Infectar los dispositivos con *malware*.** Alguien que acceda a nuestra red podría instalar *malware* en los dispositivos conectados a la misma lo que puede repercutir gravemente a nuestra seguridad.
- **Disminución del ancho de banda.** Las conexiones tienen una capacidad determinada, el ancho de banda, que se reparte entre los dispositivos que

4

estén conectados, de forma que cuantos más equipos se conecten, más lento será el intercambio de información, llegando a ser imposible usar Internet: las páginas web tardan demasiado en cargar o los videos de YouTube no se visualizan con normalidad. Dependiendo del número de intrusos y del uso que hagan de nuestra red podemos llegar a perder la conexión.

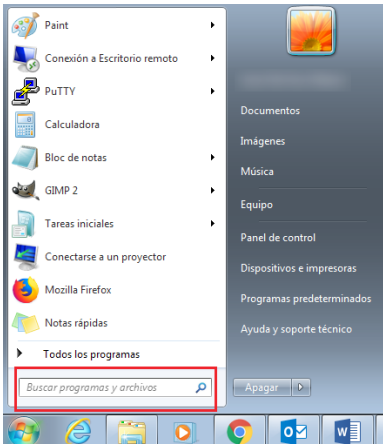
Sabiendo todo lo que un atacante puede hacer desde nuestra red es importante que la protejamos de manera correcta. Comenzamos.

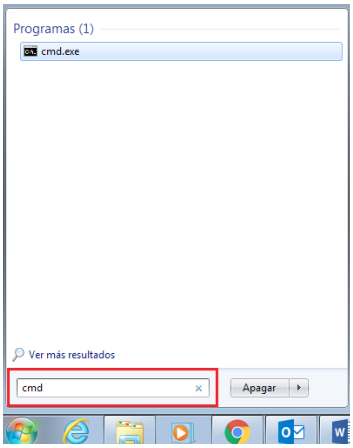
"[...]en primer lugar, será necesario conocer la dirección IP que nos da acceso al *router* [...]"

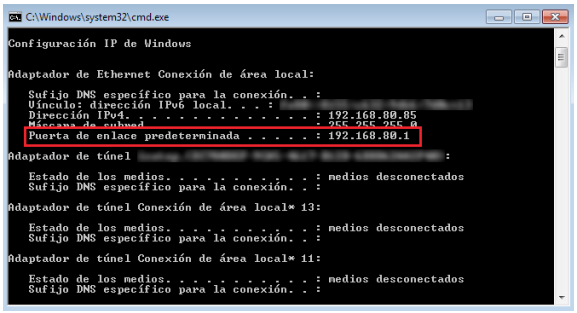
4.2. ¿Cómo acceder a la configuración del *router*?

Para llevar a la práctica esta acción será necesario, en primer lugar, conocer la dirección IP[6] que nos da acceso al *router*. Se puede saber de varias formas, nosotros recomendamos seguir los siguientes pasos para el caso de ordenadores Windows:

Botón de **Inicio** >> (en el cuadro donde dice "Buscar programas y archivos") escribir **«cmd»** >> Pinchar en el resultado >> Escribir **«ipconfig»** >> buscar la **«Puerta de enlace»**





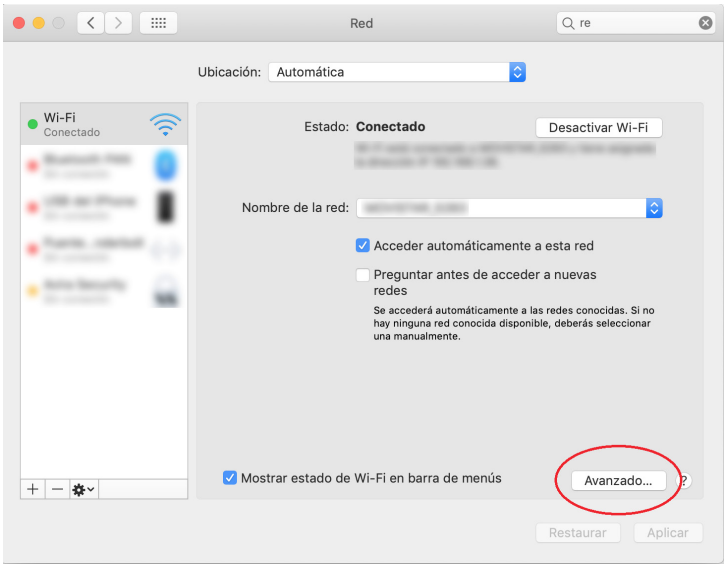


6. Una dirección IP (del acrónimo inglés IP para *Internet Protocol*), es un número único e irrepetible con el cual se identifica a todo sistema conectado a una red.

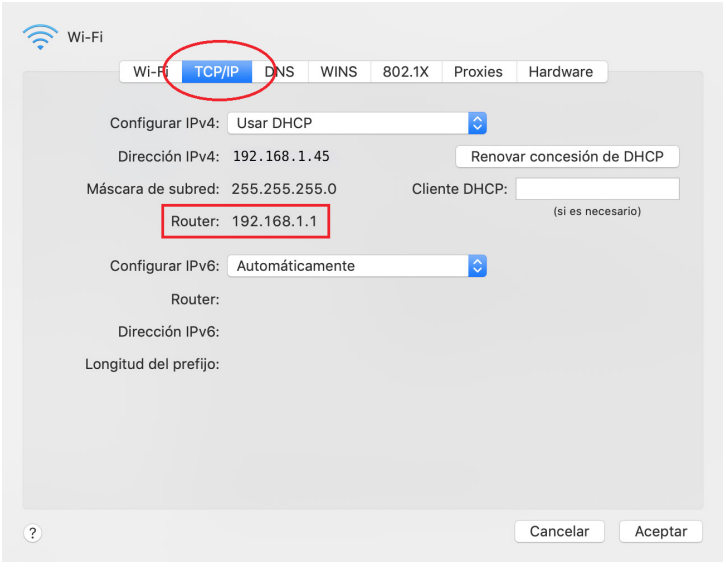
4

En el caso de ordenadores con sistema operativo **MAC OS,** los pasos que hay que seguir para saber la puerta de enlace, son los siguientes:

1 Acceder al icono de la manzana (parte superior izquierda de la pantalla), y ver las preferencias del sistema, acceder a Red, seleccionar en este caso wifi e ir a la configuración avanzada.



2 Por último habría que seleccionar la pestaña TCP/IP



4

Una vez que contamos con la dirección IP del *router*, necesitaremos de un navegador web para poder acceder al dispositivo, así como las credenciales de acceso que podrás encontrar bien en el manual del *router* o bien, en la pegatina que viene en su base o parte trasera. Una última opción sería consultar directamente al fabricante cuál es dicha contraseña:

4.3 Medidas de seguridad básicas

Una vez contamos con acceso al *router*, podremos fijar nuestra actividad en implementar una serie de medidas de seguridad básicas como las que se exponen a continuación.

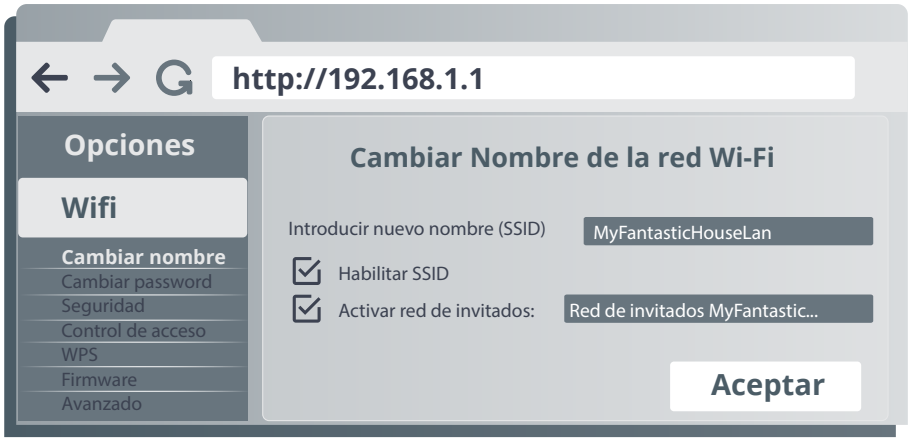
4

4.3.1 Cambiar la contraseña de acceso al *router*

Para poder cambiar la contraseña que permite el acceso a tu *router*, en primer lugar hay que buscar la opción de configuración que permite cambiar la contraseña por defecto. Hay que tener en cuenta que cada dispositivo puede contener esta opción en un lugar distinto por lo que habrá que realizar una búsqueda activa a través de los diferentes menús o disponer del manual del modelo concreto para llevar a cabo la tarea (normalmente disponible en formato digital en el paquete del dispositivo o descargable de la web del fabricante).

4.3.2 Modificar el nombre de la red wifi o (SSID)

Es muy recomendable cambiar el nombre de nuestra wifi por defecto para que no incluya ningún tipo de información que pudiera ser de utilidad para un potencial atacante (nombre de la organización, proveedor de servicios contratado, modelo de *router*, etc.).



Por lo tanto, lo mejor es quitar este tipo de información y cambiarlo por algo que no pueda ser asociado a nuestro SSID[7].

7. Del inglés *Service Set IDentifier* o identificador de paquetes de servicio, se trata del nombre que identifica una red inalámbrica y que viaja junto con cada paquete de información que es enviado desde la misma, de forma que pueda ser siempre identificado.

4

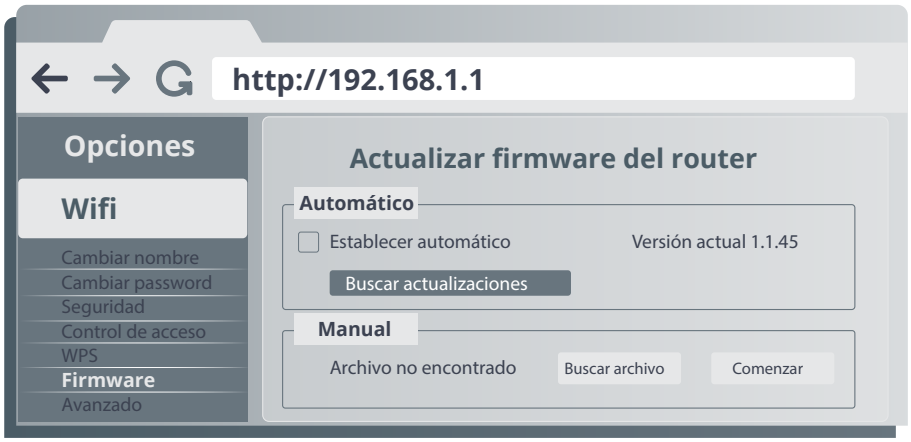
4.3.3 Contraseña de acceso a la red wifi

Otro de los principales aspectos a tener en cuenta a la hora de evitar intrusiones, es hacer uso de contraseñas de acceso a la wifi que sean lo más robustas posibles. No utilices las contraseñas por defecto que te haya proporcionado tu Proveedor de Servicios de Internet (ISP[8]), por muy segura que parezca a simple vista.

Recuerda que una contraseña robusta es aquella que utiliza un mínimo de ocho caracteres que combinen minúsculas, mayúsculas, números y caracteres especiales.

4.3.4 Actualización del *Firmware*

También deberás actualizar el firmware[9] en tu *router* cada vez que haya una nueva versión disponible. Al usar la última versión del software te aseguras de tener todos los parches de seguridad disponibles. Muchas personas no saben que sus *routers* también vienen con software, y esto es una parte muy importante para protegernos frente a posibles ataques que explotan vulnerabilidades en el software.



8. Por sus siglas en inglés *Internet Service Provider*, es la empresa que confiere conexión a Internet a sus clientes.

9 Se trata de un programa informático o software que controla las funcionalidades de un dispositivo físico o un hardware concreto como un *router*, un *Smartphone*, etc.

4

"WPA viene de las siglas *Wi-Fi Protected Access*.[...]"

4.3.5 Configurar red wifi con cifrado WPA2 o WPA3

En las configuraciones de los *routers*, normalmente se ofrecían tres modalidades de cifrado: WEP[10], WPA[11] y WPA2[12]. Posteriormente, se incorporó una más robusta y la que más se recomendaba habilitar: WPA2-PSK(AES). Sin embargo, en octubre de 2017, se descubrió una vulnerabilidad denominada «ataque KRACK **[Ref - 10]**» que permitía a un atacante interceptar, descifrar y manipular el tráfico de una red inalámbrica con el tipo de cifrado anteriormente mencionado. Ante este problema se ha desarrollado una nueva versión del protocolo WPA llamada WPA3 **[Ref - 11]**.

WPA viene de las siglas *Wi-Fi Protected* Access. Se trata de un estándar dirigido a la protección de los dispositivos, como los *routers*, de tal manera que nadie ajeno pueda acceder a los datos de manera inalámbrica. De esta forma WPA3 irá reemplazando progresivamente al WPA2. Las mejoras en autenticación, configuración o cifrado están orientadas a dificultar la acción de los atacantes, de tal forma que no puedan entrar en nuestra red.

4.3.5.1 Características del nuevo WPA3

Un punto a tener en cuenta es que WPA3 no solo ha sido presentado para redes inalámbricas personales o empresariales, sino también para el Internet de las Cosas (*Internet of Things*), también conocido como IoT.

1. Protección mejorada frente a ataques de fuerza bruta sin conexión, haciendo mucho más difícil que un atacante pueda averiguar una contraseña.
2. WPA3 Forward Secrecy. Evitará que un atacante pudiera descifrar el tráfico capturado, incluso aunque hubieran conseguido la clave en otra ocasión.

---

10 *Wired Equivalent Privacy* (WEP), en español Privacidad equivalente a cableado, es el primer mecanismo de seguridad de cifrado incluido en el estándar IEEE 802.11 para redes *Wireless*.

11 *Wi-Fi Protected Access* (WPA), en español Acceso Wi-Fi protegido, es un sistema desarrollado como una mejora de seguridad que corrigiera las deficiencias del sistema previo, WEP.

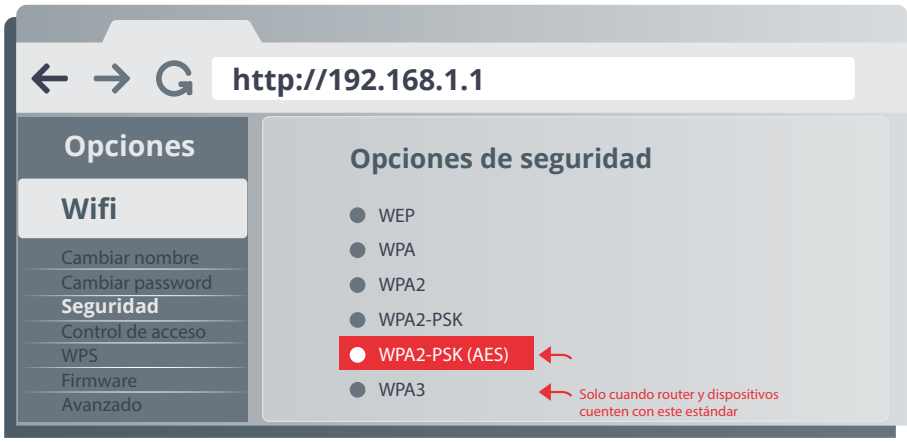
12 WPA2 (*Wi-Fi Protected Access* 2), en español Acceso Wi-Fi protegido 2, a su vez es un sistema que se creó para corregir las deficiencias del sistema previo, WPA.

4

3. Protección de redes públicas abiertas. Aunque la seguridad haya sido reforzada a través de cifrado de datos individualizado, cifrando el tráfico inalámbrico entre nuestros dispositivos y el punto de acceso wifi. La conexión a redes abiertas es una práctica desaconsejada.

4. Cifrado fuerte para redes sensibles. Ofreciendo a las redes wifi que controlan información confidencial proteger las conexiones con un cifrado más robusto, cuya clave pasa de de 128 a 192 bits. Cuanto mayor sea la clave, más difícil será romper el cifrado.

Lo que no se debe tener configurado bajo ningún concepto es el cifrado WEP, ya que es muy inseguro y alguien con los conocimientos necesarios podría robar la contraseña de la red wifi en poco tiempo. Afortunadamente, los routers más modernos, no suelen traer configurada esta opción por defecto, no obstante, es importante revisarlo.



A media que existan más dispositivos que incorporen el estándar WPA3, ésta será la elección que se deberá seleccionar.

4.3.6 Desactivar WPS

Se trata de un mecanismo que facilita la conexión de dispositivos con nuestro *router* a través de un código PIN[13] de 8 dígitos. El dispositivo que se quiere conectar a la wifi debe transmitir el código numérico al *router* y éste a cambio le enviará los datos para acceder a la red.

13 Por sus siglas en inglés *Personal Identification Number*, compuesto por al menos 4 cifras, es un número de identificación personal que funciona como sistema de seguridad de acceso.

4

"[...] mediante la creación de una red de invitados, a través de una red inalámbrica evitaremos que se tenga acceso a la red local [...]"

Tener activada esta opción implica una nueva forma de conexión que podría ser utilizada por un atacante para acceder a nuestra red wifi, ya que el tiempo que se necesita para averiguar un PIN de 8 dígitos es mucho menor que el que necesitaría para averiguar una contraseña WPA2-PSK(AES) configurada en la red.

Por lo tanto, si queremos mantener la red wifi segura, deberemos renunciar a este tipo de utilidad, desactivando el WPS.

4.3.7 Red wifi para invitados

Existen modelos de *routers* que crean una red inalámbrica separada de la red local y conocida como red de invitados.

De esta manera, mediante la creación de una red de invitados, a través de una red inalámbrica evitaremos que se tenga acceso a la red local, así como a los datos que aquí se albergan, evitando potenciales infecciones mediante la propagación de virus, *malware* o una fuga de información.

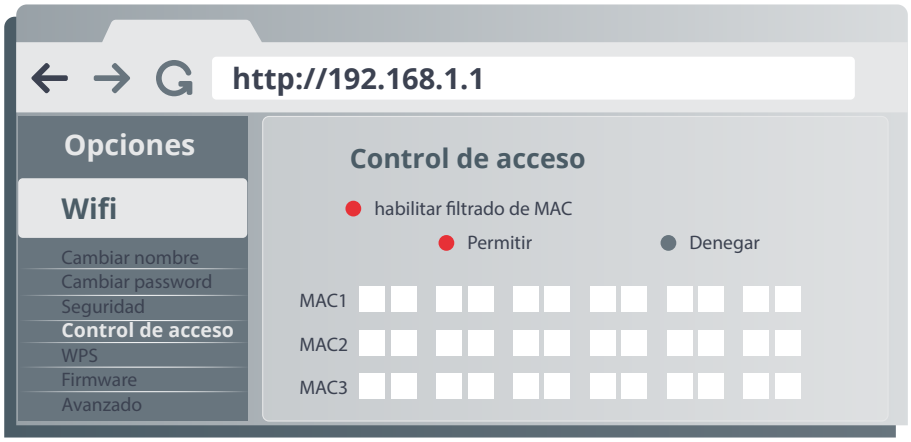
Para poder crearla, necesitaremos acceder a las opciones de **conectividad Wireless**, es decir, los ajustes de nuestra red wifi. Una vez dentro, y dependiendo del modelo de *router*, deberemos buscar el ajuste ***GuestWifi / Virtual Acces Point***, que nos permite crear un segundo punto de acceso a nuestra red local. Deberemos configurar un **SSID** diferente con una contraseña alternativa a las que tenemos, tanto para el acceso al *router* como para el acceso a la red wifi local.

4

4.4. Medidas de seguridad complementarias

4.4.1 Habilitar el filtrado por dirección MAC

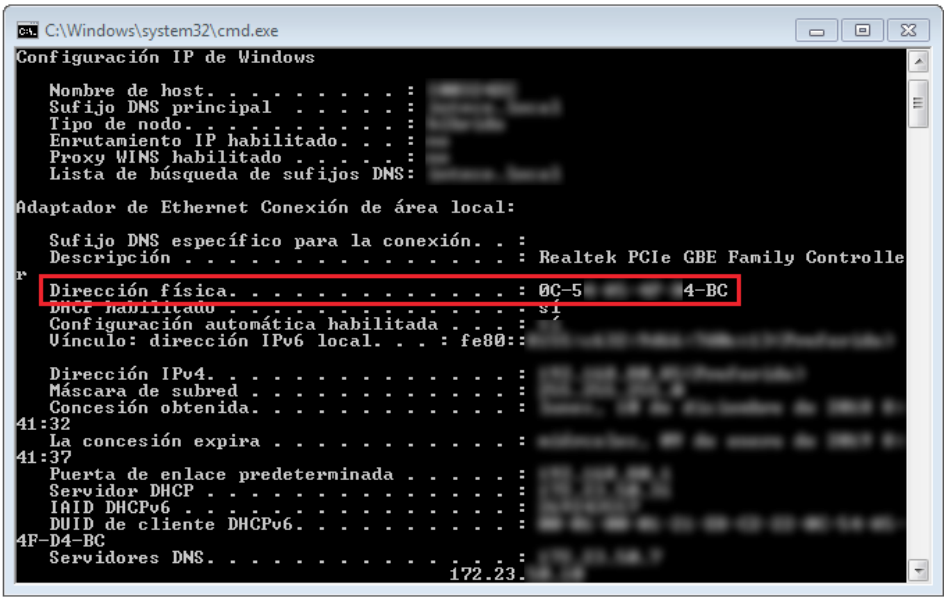
Mediante este mecanismo se pretende que únicamente las direcciones MAC que se encuentren incluidas en el *router* puedan conectarse a la red. Esta dirección es un identificador único asociado a un dispositivo concreto como un portátil o un *smartphone*.



Por lo tanto, habrá que incluir las direcciones que entendamos como oportunas en nuestro *router* y para ello deberemos acceder a las opciones en el dispositivo para establecer este control de acceso.

Como paso previo, hemos de conocer la dirección MAC de los diferentes dispositivos que queramos añadir, bien sean ordenadores, teléfonos móviles, tablets, etc.

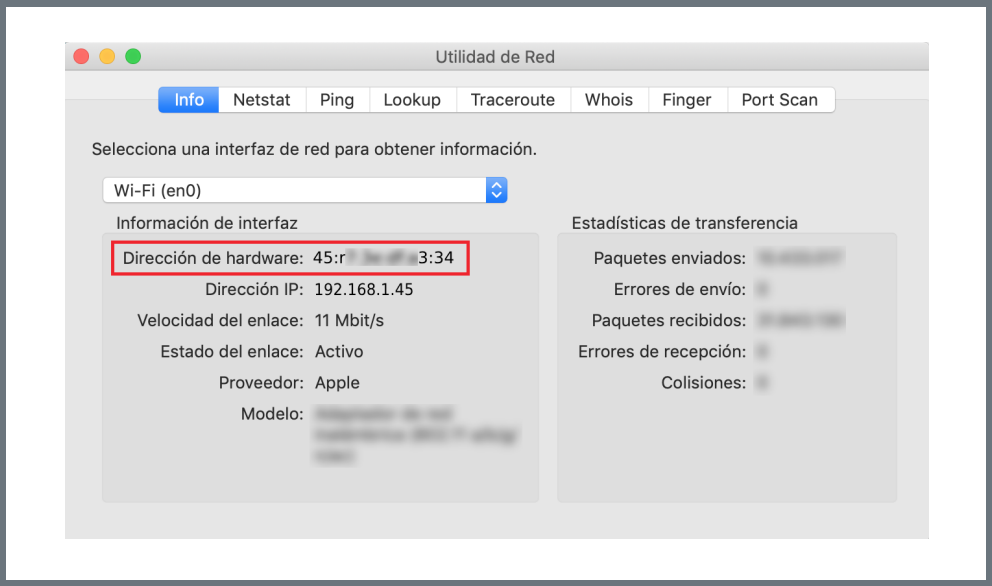
En el caso de dispositivos con sistema operativo Windows obtendremos la dirección MAC a través de la consola de MS-DOS haciendo uso del comando «ipconfig /all». En este caso, deberemos buscar el campo «dirección física».



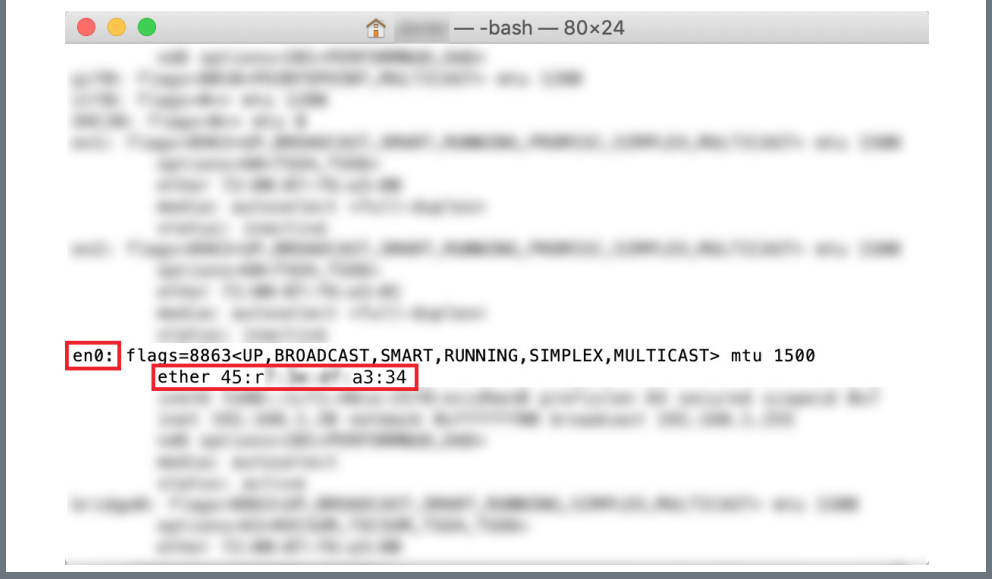
4

En el caso de dispositivos con sistema operativo Mac OS, se puede hacer de dos formas:

» Bien accediendo a las «Utilidades de Red»:



» Bien a través de un terminal haciendo uso del comando «ifconfig». El «interfaz en0» suele ser el que se utiliza para conectarse a la wifi.



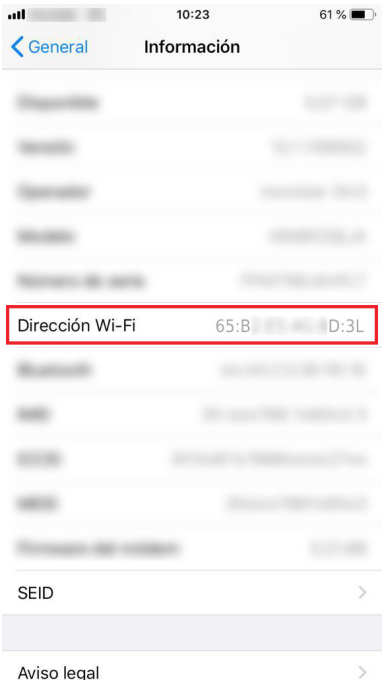
4

Los pasos necesarios para saber la dirección MAC en un móvil **Android** son los siguientes:

Menu >> Ajustes Sistema >> Información del Teléfono >> Estado >> Dirección Mac de la red Wi-Fi:

Los pasos necesarios para saber la dirección MAC en un móvil **iPhone** son los siguientes:

Ajustes >> General >> Información >> ver el apartado **"Dirección wifi":**



4.4.2 Reducir los rangos de direcciones IP permitidas

Si siempre vamos a tener los mismos equipos conectados a la red, podemos utilizar la opción de deshabilitar el funcionamiento automático del servicio DHCP[14] en el router que se encarga de asignar direcciones IP a cada equipo conectado a la red.

Esto nos obligará a tener que configurar los valores de forma manual en todos los dispositivos que tengamos en casa, pero puede aportar un grado más de seguridad. También podemos jugar con el rango de direcciones IP permitidas y restringirlo hasta los valores que queramos evitando que queden multitud de direcciones libres.

14 Por sus siglas en inglés *Dynamic Host Configuration Protocol* (en español protocolo de configuración dinámica de host), se trata de un protocolo de red mediante el cual un servidor asigna dinámicamente una dirección IP (y el resto de elementos de configuración de la red), a cada dispositivo que se conecta a la red.

4

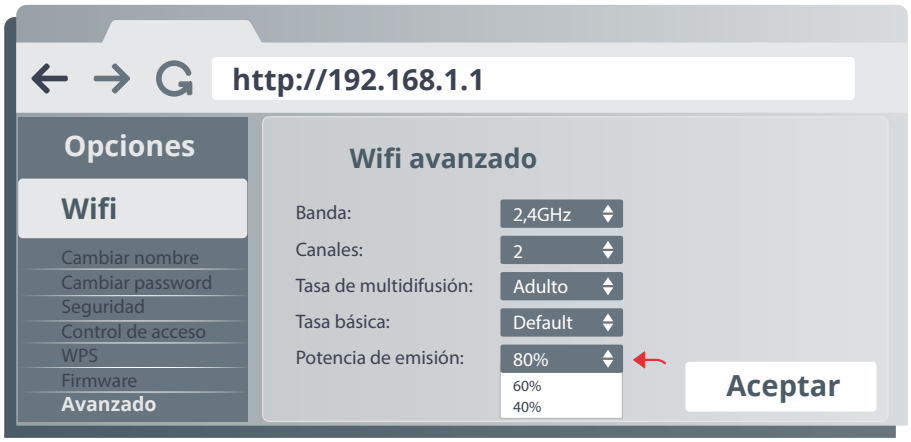
Es muy sencillo de hacer. Solo hay que buscar en el *router* la opción dentro de la configuración de la LAN en la que ponga algo similar a «Start IP Address/End IP Address» y ahí especificar los valores deseados (por ejemplo de la IP 192.168.1.33 a la 192.168.1.35, lo que nos permitiría conectar tres equipos a la red).

4.4.3 Limita la potencia de emisión de las antenas

Puede parecer obvio, pero es el método más eficaz para evitar una intrusión o el uso no permitido de tu red inalámbrica. Si no llega la señal, difícilmente alguien podrá localizar tu red y mucho menos conectarse a ella.

> " Si no llega la señal, difícilmente alguien podrá localizar tu red y mucho menos conectarse a ella."

La mayoría de los *routers* permiten gestionar de algún modo la potencia emitida por las antenas y así manejar el radio de cobertura de la red de forma aproximada. Lo habitual es que nos encontremos con alguna opción en la que se nos permita variar el porcentaje de nivel de señal o la potencia transmitida.



Aquí debemos procurar bajar la intensidad para que sigamos pudiendo conectarnos a la red dentro de casa, pero para que la potencia decaiga mucho fuera de ella. Podemos ir comprobándolo simplemente moviéndonos con el móvil por la casa y sus alrededores y viendo qué cobertura wifi tenemos.

4.4.4 Deshabilitar la administración remota

La administración remota sirve para que podamos configurar nuestro *router* fuera de nuestra red privada como por ejemplo desde la red wifi del domicilio de un familiar. Esta opción es conveniente tenerla deshabilitada, ya que de esta forma evitamos que alguien pueda conectarse a nuestro *router* desde Internet.

4.4.5 Control de equipos en la red

Los *router* cuentan con una opción en la que muestran los dispositivos conectados a la red. Accediendo a esta sección de la página de configuración podemos conocer un listado de los dispositivos conectados en tiempo real.

4.4.6 Deshabilita UPnP

También habrá un ajuste en tu panel de administración para UPnP siglas en inglés de *Universal Plug and Play*. Esto le permite a los dispositivos en la red como computadoras, impresoras, y otros dispositivos a descubrirse entre ellos mismos dentro de la red. Esto puede introducir riesgos de seguridad, y debe deshabilitarse si la opción está presente.

4.4.7 Apagar el *router*

En los horarios en que no vayas a utilizar tu conexión a Internet o en periodos de tiempo en los que no te encuentres en casa, se recomienda apagar el *router*. Es la mejor garantía de que nadie se conectará.

4.4.8 Otras medidas

Existen otras medidas de seguridad como utilizar sistemas IDS[15] e IPS[16], pero con todas estas medidas, nuestra red wifi corporativa será muy segura, rápida y estable. No debemos de complicarlo todo hasta el extremo de que utilizar la red sea un proceso tedioso y lleno de problemas, debemos de tratar de conseguir una red inalámbrica lo más segura posible, pero manteniendo las facilidades que éstas nos brindan, utilizando adecuadamente los sistemas de autentificación y configurando correctamente los equipos de red.

15 Un sistema de detección de intrusiones (o IDS por sus siglas en inglés *Intrusion Detection System*), basa su funcionamiento en el análisis de tráfico de red para detectar accesos no autorizados a un equipo o a la propia red.

16 Un sistema de prevención de intrusos o IPS (por sus siglas en inglés *Intrusion Prevention System*), es un *software* que controla los accesos a la red.

5 REFERENCIAS

[Ref - 1]. **¿Qué productos protegen las comunicaciones de tu negocio? –** https://www.incibe.es/protege-tu-empresa/blog/productos-protegen-las-comunicaciones-tu-negocio

[Ref - 2]. **Glosario de términos de ciberseguridad. Denegación de servicio – Pág. 20 –** https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf

[Ref - 3]. **Glosario de términos de ciberseguridad. Ataque de fuerza bruta – Pág. 9 –** https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf

[Ref - 4]. **Antes pyme con contraseñas fuertes que sencillas –** https://www.incibe.es/protege-tu-empresa/blog/antes-pyme-con-contrasenas-fuertes-que-sencillas

[Ref - 5]. **Contraseñas. Políticas de seguridad para la pyme –** https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/contrasenas.pdf

[Ref - 6]. **Dos mejor que uno: doble factor para acceder a servicios críticos –** https://www.incibe.es/protege-tu-empresa/blog/dos-mejor-uno-doble-factor-acceder-servicios-criticos

[Ref - 7]. **Actualización de Software. Políticas de seguridad para la pyme –** https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/actualizaciones-software.pdf

[Ref - 8]. **¿Has revisado tu nivel de seguridad? Utiliza las auditorías de sistemas –** https://www.incibe.es/protege-tu-empresa/blog/has-revisado-tu-nivel-seguridad-utiliza-las-auditorias-sistemas

[Ref - 9]. **Ataque DDoS deja fuera de servicio a múltiples sitios como PlayStation Network y Twitter –** https://www.incibe-cert.es/alerta-temprana/bitacora-ciberseguridad/ataque-ddos-deja-fuera-servicio-multiples-sitios-playstation

[Ref - 10]. **Key Reinstallation Attacks. Breaking WPA2 by forcing nonce reuse –** https://www.krackattacks.com/

[Ref - 11]. **WPA3, la mayor actualización de seguridad en redes Wi-Fi desde hace más de una década –** https://www.incibe-cert.es/blog/wpa3-mayor-actualizacion-seguridad-redes-wi-fi-hace-mas-decada

GOBIERNO DE ESPAÑA
MINISTERIO DE ECONOMÍA Y EMPRESA

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

protege tu empresa