INSTITUTO NACIONAL DE CIBERSEGURIDAD

GESTIÓN DE LA PRIVACIDAD, IDENTIDAD DIGITAL Y REPUTACIÓN ONLINE EN INTERNET

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

INSTITUTO NACIONAL DE CIBERSEGURIDAD

017

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

017

MÓDULO 9

Conexiones seguras

ÍNDICE

1. Redes wifi

En este capítulo, hablaremos sobre la conectividad inalámbrica más conocida y usada por los usuarios, las redes wifi. La palabra wifi (incluida en el diccionario de la RAE), proviene de la marca registrada Wi-Fi, una organización que promueve y certifica la tecnología y productos wifi. Se trata de un sistema que permite la conexión sin cables, dentro de un rango de distancia determinado, de dispositivos electrónicos. Su uso más conocido y extendido es el que nos da acceso a Internet.

Para hacer uso de este tipo de redes se necesitan, al menos, dos tipos de componentes: **el cliente**, que sería el dispositivo que solicita la conexión a la red inalámbrica (ordenador portátil, teléfono inteligente, tablet, etc.) y el **punto de acceso**, que es el dispositivo que hace posible la conexión entre el cliente y los otros dispositivos o redes, como Internet. Por ejemplo, los routers suelen hacer la función de punto de acceso entre nuestros dispositivos e Internet.

Entre las ***ventajas*** más relevantes a destacar de la conexión WI-Fi, se pueden nombrar:

1. Elimina la necesidad de cables físicos, fomentando mayor flexibilidad y movimiento.
2. La información es transferida en tiempo real.
3. Facilidad de instalación, sólo se necesita configurar el dispositivo para tener acceso.

Dentro de las redes inalámbricas y considerando el tipo de dispositivos que se conectan a ellas, podemos distinguir dos tipos principales:

- **Ad-Hoc**, red inalámbrica en la cual no existen puntos de acceso, los dispositivos realizan una conexión directa entre ellos, como Wi-Fi Direct o Bluetooth.
- **Infraestructura**, lugar donde se ubica el punto de acceso para realizar la conexión. Este es el tipo más común y el que usamos generalmente para acceder a Internet desde casa a través del router.

1.1 Riesgos inherentes a la tecnología wifi

A pesar de las ventajas y facilidades que nos ofrece el uso de las redes wifi, como hemos podido ver en el apartado anterior, existen ciertas limitaciones y riesgos que surgen del uso de estas.

Mientras que una conexión cableada solo podrá ser accesible para aquel dispositivo que se conecte mediante un cable al punto de acceso, requiriendo esto cercanía y la citada conexión física, las redes wifi poseen una naturaleza más abierta que incrementa los riesgos, ya que hace que cualquier dispositivo equipado con tecnología wifi y en un rango determinado de distancia al punto de acceso, pueda conectarse o intentar realizar la conexión.

Además de los riesgos asociados al uso de las redes en general, incluyendo las cableadas, dentro de los riesgos o amenazas a los que las redes wifi se enfrentan de manera específica, podemos destacar las siguientes:

- **Denegación de servicio (DoS):** se trata de la realización de un elevado número de intentos de conexión o comunicación, que la red inalámbrica, y sus componentes, se verían sobrecargados y serían incapaces de atender a todas de manera simultánea, por lo que incluso los usuarios legítimos no podrían hacer uso de la red inalámbrica afectada.

- ***Man-in-the-middle***: este tipo de amenaza consiste en que el atacante se sitúa entre emisor y receptor, es decir, entre cliente y punto de acceso. Se basa en que el atacante se sitúe así, para interceptar las comunicaciones de manera directa o a través de la suplantación de una de las partes.

- **Ataques por fuerza bruta**: este ataque consiste en acceder a una red protegida con contraseña, probando todas las combinaciones de contraseñas posibles hasta dar con la correcta. Aunque manualmente esto sería algo impracticable, los ciberdelincuentes usan herramientas que realizan esta labor sin descanso y que podrían acertar una contraseña en minutos u horas.

- ***Fugas de información de ubicación***: en las redes wifis públicas, algunos dispositivos ofrecen información sobre la ubicación de la persona usuaria, este

hecho puede ser aprovechado por delincuentes para perseguir los movimientos de la persona conectada.

- ***Eavesdropping**:* esta amenaza es una práctica consistente en la 'escucha' o captura de paquetes de tráfico, interceptando la información que se envía dentro de la red inalámbrica. Si estas comunicaciones no están cifradas, un ciberdelincuente podría acceder a toda la información que se transmite, incluidas comunicaciones privadas y contraseñas de acceso.

- **MAC *Spoofing*:** este método trata de evitar una de las medidas de seguridad usadas en las redes wifi, en las que sólo se permite acceso a la misma a dispositivos con una determinada MAC, que no es más que un identificador único usado por los dispositivos que tienen acceso a redes. El método en sí suplanta una MAC legítima para ganar acceso a la red con un dispositivo no autorizado.

- ***Puntos de acceso falso (Rogue Access Points):*** dispositivo que es instalado en una red sin el conocimiento de las personas administradoras, configurando los puntos de acceso para que se conecten a ellos, pudiendo acceder de este modo a datos personales.

1.2 Medidas de seguridad para las redes wifi

Para mitigar los riesgos a los que nos exponemos en el mundo digital actual con el uso de las redes inalámbricas, existen una serie de medidas de seguridad recomendadas. Aunque en el siguiente capítulo entraremos en detalle en algunas de ellas para aprender cómo configurar nuestra red inalámbrica de manera segura, a continuación, mostraremos un pequeño resumen de cada una de ellas:

- **Cambiar la contraseña de acceso al router.** La configuración por defecto de los routers ha sido y sigue siendo uno de los principales puntos débiles de las redes inalámbricas. Muchos fabricantes han optado por usar contraseñas y usuarios genéricos como 'admin' y '1234' para acceder al router, abriendo la puerta a que un atacante pueda cambiar las configuraciones del punto de acceso. Es por ello, que se recomienda cambiar estas credenciales accediendo a nuestro router e instalando una contraseña

más robusta, usando letras minúsculas, mayúsculas, números y caracteres especiales.

- **Modificar el nombre de la red wifi o (SSID).** En ocasiones, el nombre del punto de acceso wifi, conocido como SSID, puede dar pistas a un atacante sobre el modelo del router y del operador de Internet facilitando así su labor, por lo que es recomendable cambiar el nombre que trae por defecto.

- **Contraseña de acceso a la red wifi.** Aunque la contraseña que viene por defecto en nuestros routers parezca muy segura y compleja, es posible que haya sido generada con un algoritmo o siguiendo un patrón que los ciberdelincuentes podrían descubrir. Es por ello que se recomienda cambiar la contraseña por alguna que generemos nosotros mismos y que sea lo más compleja posible.

- **Actualización del *firmware* del router.** Nuestros routers también tiene su propio *software* o sistema operativo, por lo que al igual que en cualquier otro dispositivo, es altamente recomendable actualizarlo siempre que exista una nueva versión disponible.

- **Configurar red wifi con cifrado WPA2 o WPA3**. Dentro de la configuración de nuestros routers encontraremos diferentes modalidades de cifrado que pueden ser WEP, WPA, WPA2 y WPA3. Estos cifrados están destinados a que la información que se transmite no sea accesible para terceros no autorizados. A día de hoy, solo WPA3 está libre de vulnerabilidades, por lo que es la primera opción si nuestro router lo permite. Si no fuera el caso, WPA2 es la siguiente configuración más segura. Se desaconseja totalmente el uso de WEP por ser el menos seguro.

- **Desactivar WPS.** La funcionalidad WPS trata de facilitar el acceso a nuestra red mediante la posibilidad de conexión con un código pin de ocho dígitos. Aunque podría facilitarnos al acceso a nosotros o nuestros invitados, también puede facilitar el acceso a un potencial atacante, por lo que es preferible mantener esta funcionalidad desactivada.

- **Apagar el router.** Durante los horarios o épocas en las que no se vaya a usar la red inalámbrica, es recomendable apagar el router. Ésta es la única medida que garantiza al 100% que nadie tratará de acceder a la red wifi.

Adicionalmente, existen algunas medidas de seguridad más avanzadas con las que se trata de dar una vuelta de tuerca más a la seguridad de las redes wifi, y como consecuencia, aumentar la privacidad de los datos que transmitimos a través de ellas.

- **Habilitar el filtrado por dirección MAC.** Consiste en proporcionar acceso a una red wifi únicamente a dispositivos específicos, basándonos en su identificador único de red, conocido como MAC. Todos los router permiten configurar este aspecto para que solo se conecten a la red wifi los dispositivos que nosotros indiquemos.

- **Reducir los rangos de direcciones IP permitidas.** Cuando son los mismos dispositivos los que están conectados a una red, además del filtrado MAC, es posible deshabilitar el servicio DHCP del router, que se encarga de asignar direcciones IP de manera automática a los dispositivos. Como consecuencia, habrá que configurar de manera manual cada uno de los dispositivos conectados y asignar la IP deseada, y, por último, configurar en el router el rango específico de IP que tendrá autorizado el acceso a la red.

- **WIPS (Wireless Intrusion Prevention System).** Este sistema de prevención de intrusión inalámbrica, es un hardware de red que protege a las redes inalámbricas y actúan detectando, bloqueando y notificando posibles amenazas que puedan ir apareciendo.

- **Limitar la potencia de las antenas.** Aunque a veces pasa desapercibido, este método es muy eficaz para reducir el rango en el que podemos acceder a la red wifi, y, por lo tanto, el rango desde el que un atacante podría intentar el acceso a la misma también se limita, por lo que resultará más complicado que se conecte a nuestra red.

- **Deshabilitar la administración remota**. Esta funcionalidad sirve para que el portal de configuración del router sea accesible desde otras redes, por lo

que es recomendable deshabilitarlo, permitiendo acceso a dicha configuración solo a los dispositivos conectados a la propia red.

- **Control de equipos en la red.** La mayoría de los routers nos ofrecen dentro de su portal de configuración una lista de los dispositivos conectados en tiempo real, resulta muy útil para asegurar que no existe un intruso en la red.

- **Deshabilita UPnP.** Dentro del portal de configuración es posible que encontremos un ajuste para activar la función UPnP, que permite que los dispositivos dentro de la red puedan comunicarse entre sí. Es recomendable desactivarlo, ya que incrementaría los riesgos en caso de sufrir un ataque en la red wifi.

En el apartado 2 de este módulo, encontrarás más detalle sobre cómo configurar el router adecuadamente para prevenir todos estos riesgos.

1.3 Redes wifi públicas, ¿sí o no?

Las redes públicas o abiertas, son aquellas a las que nos podemos conectar de manera gratuita mediante un proceso de autenticación o facilitando una contraseña de acceso para conectarnos. Algunas de ellas, incluso no están protegidas por ningún tipo de contraseña. Estas redes se suelen encontrar en centros comerciales, cafeterías, restaurantes, bibliotecas, hoteles, etc.

Cuando nos conectamos a una red pública, por norma general, no conocemos al administrador ni las medidas de seguridad que han sido aplicadas, al igual que no conocemos a los demás usuarios de la red conectados. En consecuencia, existen ciertos riesgos a los que nos enfrentamos al usar este tipo de redes, ya que al carecer de cifrado (WEP, WPA, WPA2, WPA3) la información viaja de manera legible para el administrador u otros usuarios de la red.

Así pues, estamos exponiéndonos a robo de información transmitida, por lo que es recomendable evitar el uso de dichas redes en caso de no tener necesidad.

Aunque es recomendable no hacer uso de redes públicas, ya que los datos pueden ser interceptados por personas malintencionadas , pueden existir momentos en los que nos vemos en la necesidad de utilizarlas para obtener algún tipo de

información, descargar algún archivo de nuestro correo o simplemente contactar con alguien. En esta infografía te damos los principales consejos a seguir para evitar que esta conexión se convierta en una mala experiencia.

2. Cómo proteger nuestra conexión wifi

Mantener nuestra red wifi sin contraseña o abierta, significa que cualquier persona puede hacer uso de ella para acceder a Internet. Aunque, quizás queramos ser generosos y compartir nuestra conexión, hemos de entender que esto implica unos riesgos, que vamos a enumerar a continuación:

- **Reducción del ancho de banda.** La velocidad de nuestra conexión se verá afectada cuantos más dispositivos se conecten, y en casos extremos, podrían llegar al límite y, como consecuencia, no permitir que nuestros dispositivos se puedan conectar.
- **Robo de la información transmitida**. Cuando una conexión wifi no está protegida por contraseña, no solo significa que el acceso a ésta es libre, sino que además implica que la información que trasmitimos a través de ella no está cifrada, por lo que podría ser interceptada, incluyendo datos personales o contraseñas a personas que dispongan de conocimientos suficientes para extraer información sensible.
- **Exposición de dispositivos personales conectados**. Los dispositivos conectados como cámaras de seguridad, sistemas de domótica u otros , suelen estar más expuestos debido en ocasiones a la falta de medidas de seguridad que incorporan, poniendo en riesgo información sensible y personal que utilizan para su correcto funcionamiento.
- **Responsabilidad legal.** Nuestro contrato con el proveedor de Internet conlleva unas responsabilidades legales, y una de ellas es que somos responsables de cualquier acción realizada desde nuestra conexión. Por lo tanto, como titulares del contrato tendremos que responder ante la justicia en caso de que alguien que esté usando nuestra conexión cometa algún delito cibernético.

2.1 Configurando router y WLAN de forma segura

Nuestros routers son los dispositivos encargados de darnos acceso a Internet, trabajando de manera silenciosa y continua, manteniendo nuestra red WLAN (inalámbrica) activa para que podamos acceder en todo momento a través de nuestros dispositivos electrónicos, como teléfonos, tablets, portátiles, televisores inteligentes, etc.

Desafortunadamente, ese trabajo que realizan a la sombra hace que en ocasiones pasen desapercibidos y solo nos acordemos de ellos cuando nuestra conexión no funciona correctamente. Sin embargo, no debemos olvidar la importancia que tienen, no sólo para conectarnos a Internet, como comentábamos anteriormente, sino que también juegan un papel fundamental en la protección de nuestros datos, y, por lo tanto, de nuestra privacidad.

Así pues, y conociendo los riesgos a los que estamos expuestos por el simple hecho de conectarnos a Internet y en especial por el uso de redes wifi, es de vital importancia configurar de manera segura nuestros routers y la red inalámbrica que nos proporcionan.

Para comenzar, deberemos acceder a la página de configuración de nuestro router, para lo que encontramos las instrucciones y las credenciales generalmente en el mismo router. Tenemos que tener en cuenta que según el modelo y el fabricante del router, esta configuración puede variar, pero los menús principales son muy similares. Por norma general, este acceso se realiza escribiendo la dirección IP del router en nuestro navegador, como si de una página web a la que queremos acceder se tratase, y usando las credenciales que se nos muestren en el router o en las instrucciones del mismo. Las direcciones más usadas son 192.168.1.1 o 192.168.0.1.

En el capítulo que empezaremos a continuación, se dividen las configuraciones a realizar en dos: aquellas dedicadas a la red WLAN o wifi que nuestro router crea, y a la configuración del router en sí para hacerlo lo más seguro posible.

2.2 Configuración de la red WLAN

En este apartado, detallaremos cómo hemos de configurar nuestra red inalámbrica de forma segura, evitando así accesos no autorizados e indeseados que puedan comprometer nuestra privacidad. En el caso de nuestro router de ejemplo, tenemos una pestaña dedicada 'Wi-Fi' donde encontraremos los ajustes que queremos llevar a cabo:

- **Modificar el nombre de la red wifi o (SSID).** En ocasiones, el nombre del punto de acceso wifi (conocido como SSID) puede dar pistas a un atacante y facilitar su labor, por lo que es recomendable cambiar el nombre por defecto. Para ello debemos de

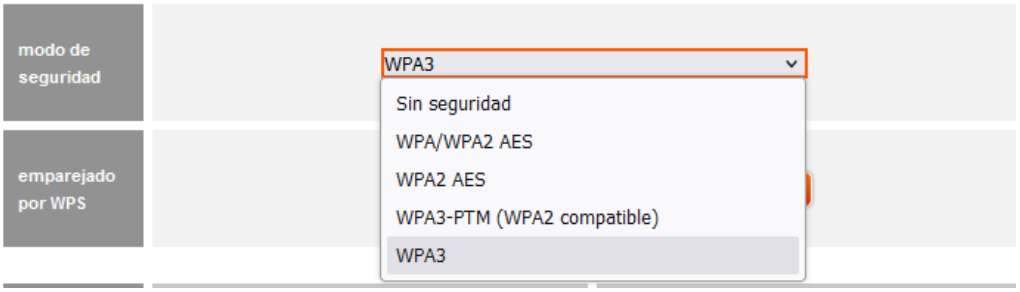
ir a la opción *Configuración del Wi-Fi*, luego modificar el *nombre de Wi-Fi* y posteriormente *guardar*.

- **Contraseña de acceso a la red wifi.** Aunque la contraseña que viene por defecto en nuestros routers parezca muy segura y compleja, es posible que haya sido generada con un algoritmo o siguiendo un patrón que los ciberdelincuentes podrían descubrir. Es por ello que se recomienda cambiar la contraseña por alguna que generemos nosotros mismos y que sea lo más compleja posible. Los pasos a seguir son: Acceder a *Configuración del Wi-Fi* > *clave Wi-Fi inteligente*. A continuación, habrá que escribir la nueva clave y pulsar en *guardar*.

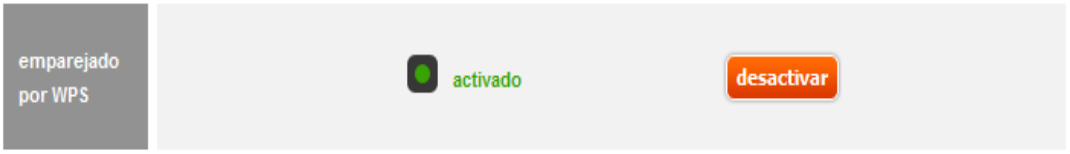
Una vez introducida la nueva contraseña, nos aparecerá en la parte derecha del recuadro el grado seguridad que tiene, si considera que la contraseña que se está introduciendo no es lo suficientemente robusta aparecerá en rojo e indicará '*débil*',

de lo contrario, aparecerá de color verde e indicará '*robusta*', tal y como se aprecia en la imagen anterior.

- **Configurar red wifi con cifrado WPA2 o WPA3**. Dentro de la configuración de nuestros routers encontraremos diferentes modalidades de cifrado, que pueden ser WEP, WPA, WPA2 y WPA3. Estos cifrados están destinados a que la información que se transmite no sea accesible para terceros no autorizados. A día de hoy, solo WPA3 está libre de vulnerabilidades, por lo que es la primera opción si nuestro router lo permite. Si no fuera el caso, WPA2 es la siguiente configuración más segura.
  Para ello, debemos de ir al panel *configuración del Wi-Fi> modo de seguridad*, elegir entre las opciones del desplegable, en el caso del ejemplo será *WPA3*, y, por último, *guardar*.



- **Desactivar WPS.** La funcionalidad WPS trata de facilitar el acceso a nuestra red mediante la posibilidad de conexión con un código pin de ocho dígitos. Aunque podría facilitarnos al acceso a nosotros o nuestros invitados, también puede facilitar el acceso a un potencial atacante, por lo que es preferible mantener esta funcionalidad desactivada.
  Para ello desactivaremos esta opción en: *configuración del Wi-Fi > emparejado por WPS >desactivar*.



- **Cuenta de administración.** También como medida de seguridad, está la opción de modificar el nombre y contraseña a la hora de acceder a la configuración de la red inalámbrica.

- **Habilitar el filtrado por dirección MAC.** Cómo comentábamos dentro de los riesgos inherentes de las redes wifi, una de las medidas de seguridad usadas consiste en proporcionar acceso a una red wifi únicamente a dispositivos específicos, basándonos en su identificador único de red, conocido como MAC.

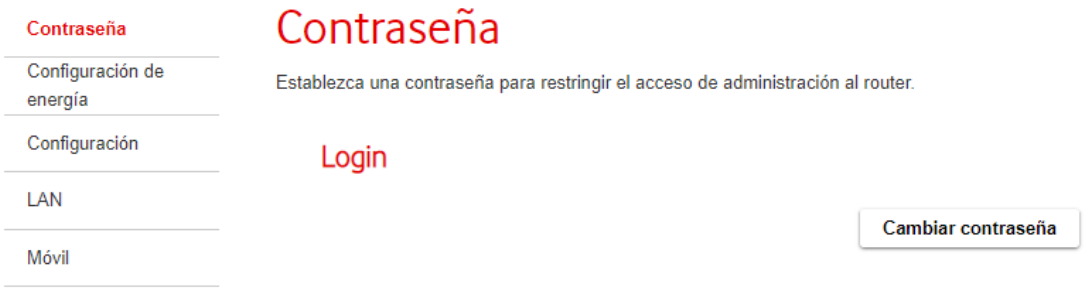
Para localizar la dirección MAC del dispositivo, dependiendo del sistema operativo, accederemos a:

- Ajustes > Acerca del teléfono > Información de estado > MAC de Wi-Fi (Android).
- Configuración > General > Acerca de > Dirección de Wi-Fi (iOS).
- Inicio > cmd > ipconfig/all > Dirección física, dentro de 'Adaptador de LAN inalámbrica'.

2.3 Configuración del router

Además de configurar nuestra red inalámbrica con los pasos explicados anteriormente, es primordial que nuestro router también esté configurado de manera segura, ya que por muy bien que protejamos nuestra red wifi, si, por ejemplo, un ciberdelincuente consigue acceder a nuestro router, todos los esfuerzos y la seguridad aplicada a la red wifi serían en vano.

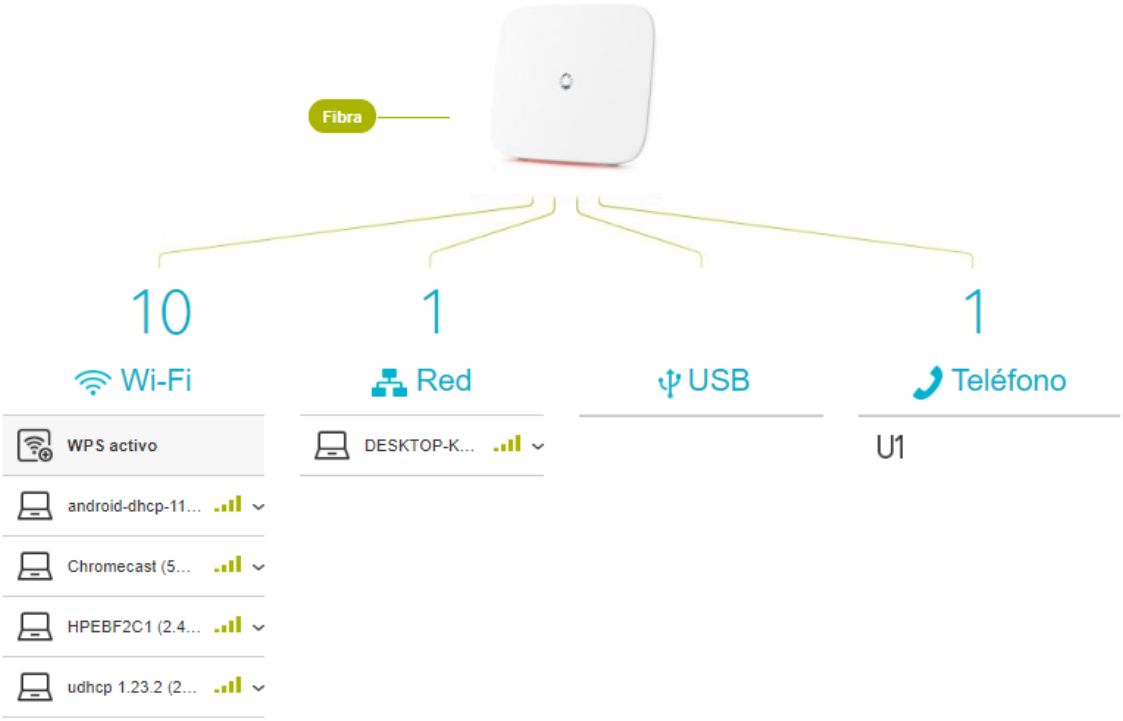
- **Cambiar la contraseña de acceso al router.** La configuración por defecto de los routers ha sido y sigue siendo uno de los principales puntos débiles de las redes inalámbricas. Como mencionábamos en el apartado anterior, muchos fabricantes han optado por usar contraseñas y usuarios genéricos como 'admin' y '1234' para acceder al router, abriendo la puerta a que un atacante pueda cambiar las configuraciones del punto de acceso. Es por ello, que se recomienda cambiar estas credenciales accediendo a nuestro router.



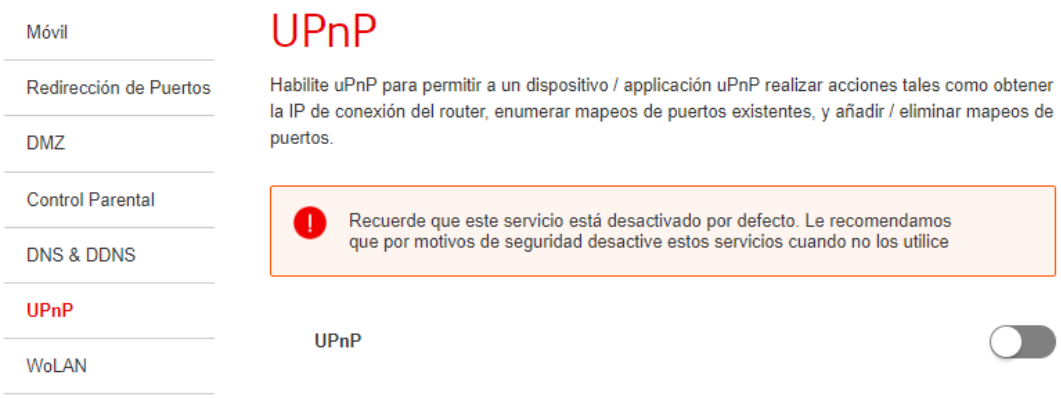
- **Actualización del *firmware* del router.** Nuestros routers también tienen su propio *software* o sistema operativo, por lo que al igual que en cualquier otro dispositivo, es altamente recomendable actualizarlo siempre que exista una nueva versión disponible. Podremos acceder a esta opción desde el menú del router, o llamando a nuestra operadora y solicitando la actualización.

- **Reducir los rangos de direcciones IP permitidas.** Cuando son los mismos dispositivos los que están conectados a una red, además del filtrado MAC, es posible deshabilitar el servicio DHCP del router, que se encarga de asignar direcciones IP de manera automática a los dispositivos. Como consecuencia, habrá que configurar de manera manual cada uno de los dispositivos conectados y asignar la IP deseada, y configurar en el router el rango específico de IP que tendrá autorizado el acceso a la Red. Quizás esta medida es un poco más avanzada para aquellos usuarios que tengan menos conocimientos técnicos, no obstante, es importante valorar su implementación.

- **Control de equipos en la red.** La mayoría de los routers nos ofrecen dentro de su portal de configuración una lista de los dispositivos conectados en tiempo real, que es muy útil para asegurar que no existe un intruso en la Red, para en ese caso, revocarle la conexión.



- **Deshabilita UPnP (Universal Plug and Play).** Dentro del portal de configuración, es posible que encontremos un ajuste para activar UPnP, que permite que los dispositivos dentro de la Red puedan comunicarse entre sí. Es recomendable desactivarlo, ya que incrementaría los riesgos en caso de sufrir un ataque en la red wifi. Otra función técnica, pero muy interesante.



- **Apagar el router.** Durante los horarios o épocas en las que no se vaya a usar la red inalámbrica, es recomendable apagar el router. Ésta es la única medida que garantiza al 100% que nadie tratará de acceder a la red wifi.

MÁS INFORMACIÓN

INCIBE tiene publicada la guía "Tu router, tu castillo", donde encontrarás todos los pasos que debes seguir para configurar el router de forma segura.

La guía explica aspectos físicos básicos del router para que te familiarices con ellos antes de comenzar con las configuraciones. También describe las principales amenazas de ciberseguridad que pueden afectar al dispositivo para que seas consciente de los riesgos a los que te expones si no tomas las suficientes medidas preventivas. Adicionalmente, muestra de manera muy visual y sencilla cómo realizar las diferentes configuraciones seguras en el router.

Descargar guía: Ver enlace

3. *Wearables*, conexiones Bluetooth y NFC

Los dispositivos *wearables* han extendido su cota de mercado en los últimos años de manera notable, convirtiéndose en uno más de los dispositivos imprescindibles para muchos usuarios, por su tamaño, facilidad de uso y funcionalidades. En este sentido, destacan los que nos ayudan a controlar nuestra salud mediante el ritmo cardiaco, niveles de oxígeno en sangre o de azúcar, o simplemente midiendo nuestro nivel de actividad y las actividades específicas que realizamos. Pulseras, relojes o auriculares inteligentes son algunos de los más comunes, pero la lista no para de crecer.

En el siguiente enlace se pueden ver la cantidad de envíos de dispositivos wereables a nivel mundial entre el año 2023 y 2027 enlace.

Pero a pesar de todas sus bondades, a veces tendemos a olvidar que, al tratarse de dispositivos inteligentes, están conectados de igual manera que un teléfono o un ordenador, por lo que toda la información que registran y a la que tienen acceso también puede estar en riesgo si no tomamos las medidas adecuadas.

3.1 *Wearables*, principales riesgos y recomendaciones

Como explicábamos anteriormente, los *wearables* son dispositivos electrónicos que podemos llevar en alguna parte de nuestro cuerpo, que se conectan por un lado a los servidores o la plataforma del fabricante a través de una aplicación, y por otro, a nuestro teléfono móvil o tablet, haciendo uso, en la mayoría de los casos, de la tecnología Bluetooth.

Esta conectividad hace que todos los datos que los *wearables* recopilan y envían estén expuestos a una serie de riesgos:

- **Seguridad de los servidores del fabricante.** Si el fabricante no dispone de unos servidores seguros, es posible que todos los datos recopilados acaben

en manos de ciberdelincuentes, y estos acaben haciéndolos públicos o vendiéndolos al mejor postor. Aunque ningún fabricante está libre de ciberataques, a priori, siempre serán más fiables los servidores de fabricantes que tengan cierto renombre.

- **Políticas de privacidad pobres o nulas.** Cuando instalamos la aplicación que recopilará los datos o durante el proceso de configuración inicial del dispositivo, se nos dará información de qué tipos de datos se van a almacenar y con qué fin. Es importante que no nos saltemos ese paso y seamos conscientes de todo el proceso que se llevará a cabo con nuestros datos privados.
  Actualmente dependiendo de país dónde nos encontremos, algunos de estos dispositivos como gafas inteligentes pueden grabar videos y audios, y en consecuencia grabar a terceras personas sin autorización, lo que conlleva un delito penal. Por este ejemplo y muchos otros es de vital importancia prestar atención a estas políticas de privacidad.

- **Permisos sospechosos.** Algunos de estos dispositivos y sus aplicaciones pueden llegar a solicitar más permisos de los estrictamente necesarios para su funcionamiento. Es recomendable asegurarse que solo le otorgamos los permisos necesarios, nunca de más. Si por ejemplo solo queremos que un *wearable* registre nuestras actividades físicas, no sería necesario que pueda acceder a nuestros mensajes de textos, archivos o contactos.

- **Localización y otros sensores.** Ya que estamos hablando de dispositivos que en su gran mayoría recogen nuestra ubicación gracias a la geolocalización mediante GPS, un ciberdelincuente puede saber exactamente dónde estamos en cada momento, si esta información no se protege correctamente. Hace unos años, se descubrió que empresas como Fitbit (empresa de pulseras inteligentes) y Strava (aplicación de corredores) permitían saber las bases secretas del ejercito de los EE.UU debido al lugar dónde se encontraban los militares.
  Para mitigar este riesgo, y evitar que un ciberdelincuente no acceda a nuestra ubicación, es importante conceder este permiso exclusivamente cuando realmente el dispositivo lo necesite para realizar la función que le vamos a encomendar. Igualmente, muchos de estos dispositivos cuentan con

cámaras o micrófonos, que podrían ser usadas para recopilar información adicional sobre nosotros.

- **Información pública.** En muchas de las aplicaciones con las que funcionan este tipo de dispositivos, existe una gran cantidad de información que se comparte de manera pública, en especial aquellas relacionas con salud y deporte, ya que están diseñadas para compartir nuestros registros por defecto con otros usuarios. Esta información, en manos inadecuadas, puede dar mucha información a ciberdelincuentes para materializar un ataque de ingeniería social personalizado, es decir, con engaños más creíbles, ya que utilizan datos verídicos sobre nosotros a los que han tenido acceso. Es importante asegurarnos de qué tipo de información estamos compartiendo y con quién, buscando las opciones de privacidad y de compartir dentro de la aplicación principal de nuestro dispositivo *wearable*.

- **Conexiones poco seguras.** La gran mayoría de estos dispositivos hacen uso de conexiones para sincronizar nuestros datos con otros dispositivos. Estas conexiones, si no están correctamente securizadas, podrían ser interceptadas por ciberdelincuentes, apoderándose así de toda la información que se está sincronizando en ese momento. Para mitigar este riesgo, es recomendable usar una tarjeta SIM propia, siempre que sea factible, y realizar las sincronizaciones en entornos seguros, evitando por ejemplo lugares muy concurridos donde la intercepción de la información pudiera llevarse a cabo y pasar desapercibida.

- **Falta de medidas de seguridad.** Para hacer este tipo de dispositivos más accesibles, muchos fabricantes se enfocan en su funcionalidad dejando de lado el apartado de seguridad. Es por ello, que no es raro encontrar dispositivos *wearables* con contraseñas por defecto muy sencillas, pocas opciones de privacidad o poca información sobre cuáles de nuestros datos se van a almacenar, dónde y cómo. Conocer qué medidas de seguridad y qué tratamiento de datos hará el dispositivo antes de adquirir o comenzar a usarlo es clave si queremos mantener nuestra información a salvo.

En conclusión, es importante que, si contamos con uno de estos dispositivos, o tenemos intención de adquirir uno, tengamos en cuenta los puntos anteriores y

apliquemos las recomendaciones dadas para mitigar los riesgos a los que nos exponemos con su uso y podamos disfrutar de ellos con tranquilidad.

3.2 Conexiones Bluetooth

El Bluetooth es una de las tecnologías inalámbricas más usadas para sincronizar y conectar dispositivos. Lleva muchos años con nosotros (fue en 1999 cuando el primer dispositivo Bluetooth fue comercializado), su uso sigue estando muy extendido y sigue mejorando para permitirnos conectar dispositivos a mayor velocidad y distancia. Aunque también ha mejorado en la seguridad durante los últimos tiempos, el uso de esta tecnología nos expone a una serie de riesgos que debemos conocer y saber cómo afrontarlos para proteger nuestra privacidad. A continuación, mostramos algunos de los más conocidos.

- *BlueSmacking*

Se trata de un ataque DoS (denegación de servicio), en el que el atacante realiza numerosas solicitudes para saturar la conexión y evitar que podamos usarla con normalidad.

- *BlueSnarfing*

Este ataque busca interceptar datos transmitidos vía Bluetooth, por lo que podría dar acceso al atacante a nuestros datos confidenciales y comprometer así gravemente nuestra privacidad, además de dar información que podría ser usada más adelante para otro tipo de ataques de ingeniería social.

- *BlueJacking*

Consiste en el envío de mensajes indeseados a través de Bluetooth, sincronizando con nuestro dispositivo sin nuestro consentimiento. Los mensajes recibidos puede ser enlaces maliciosos que infecten nuestros dispositivos con *malware* o un intento de *phishing*.

- Rastreo de ubicación

Como comentábamos en al apartado de dispositivos *wearables*, muchos de ellos usan Bluetooth y tienen acceso a nuestra ubicación, ya que los usamos para actividades deportivas o simplemente medir nuestros pasos. Un atacante con esta información podría saber exactamente dónde nos encontramos en cada momento, comprometiendo nuestra privacidad, y en algunos casos, nuestra integridad.

- Escucha de conversaciones

Ya que el uso de auriculares inalámbricos se ha extendido mucho, y todos ellos están conectados mediante Bluetooth, alguna vulnerabilidad usada por atacantes podría permitir que nuestras conversaciones sean escuchadas, comprometiendo nuevamente nuestra privacidad de manera grave.

- *Spoofing*

Aunque esta práctica no está muy extendida en estos dispositivos, es importante señalar ya que puede encontrarse el caso de que algún ciberdelincuente pueda fingir ser un dispositivo Bluetooht legítimo y acceda de manera no autorizada a nuestros datos.

3.3 Tecnología NFC

El NFC (tecnología de comunicación de campo cercano) es una tecnología de comunicación inalámbrica de alcance muy corto, para el intercambio de información entre dos dispositivos muy cercanos, con un alcance máximo aproximado de 10cm, que prácticamente han de tocarse para llevar a cabo dicho intercambio.

Esta tecnología tiene múltiples usos, como lector de DNI electrónicos o identificación personal, sincronización de dispositivos o acceso a contenidos. Sin embargo, su uso más extendido es el de la realización de pagos a través de dispositivos inteligentes que cuentan con esta tecnología. La forma de funcionamiento es exactamente la misma que las tarjetas de crédito conocidas como *contactless* (sin contacto). Sólo deberemos activar el pago mediante algún método de autentificación y acercar nuestro dispositivo al terminal de pago.

3.4 Riesgos y precauciones en el uso de la tecnología NFC

Aunque se trata de un método de comunicación muy seguro, ya que sólo actúa en un rango de distancia muy corto, también está expuesto a algunos de los riesgos inherentes de las conexiones inalámbricas.

1. **Escucha o intercepción de información.** Cuando nuestro dispositivo establece una comunicación NFC, hemos de asegurarnos que lo hacemos a otro dispositivo de confianza para evitar que la información o el pago que se transfiere llegue a un destinatario indeseado.

2. **Vulnerabilidades.** Cuando usamos la tecnología NFC con aplicaciones de pago o lectores, si estas aplicaciones no están actualizadas podrían contener vulnerabilidades que pueden ser aprovechadas por ciberdelincuentes para realizar ataques o accesos indeseados. Por ello, es importante tenerlo renovado con las últimas actualizaciones de *software*.
3. **Pérdida del dispositivo.** Ya que esta tecnología puede convertir nuestro dispositivo en un método de pago, su pérdida nos puede ocasionar graves problemas, como si de una tarjeta de crédito se tratara. Es por ello, que hemos de asegurarnos de habilitar un método de verificación doble para efectuar pagos y en caso de pérdida, desactivar las tarjetas asociadas a la mayor brevedad posible. También es recomendable revisar de manera regular los extractos de cuentas por si se percibe cualquier actividad que pueda ser sospechosa.
4. **NFC activa de manera constante.** Al igual que mencionábamos con la tecnología Bluetooth, la mejor manera de evitar todos los riesgos asociados a la misma, es desactivando la conectividad. Así pues, es recomendable que sólo activemos NFC cuando vayamos a hacer uso de ella, para evitar que alguna información sea enviada accidentalmente, o que un actor malicioso busque procesar un pago, por ejemplo, acercándose a nuestro dispositivo.

Para poder seguir disfrutando de las ventajas que nos proporciona esta tecnología, pero sin comprometer nuestra privacidad y seguridad, hemos de seguir una serie de recomendaciones que detallamos a continuación.

En esta infografía, trataremos de mostrar de manera visual las principales medidas que hemos de llevar a cabo para proteger nuestras conexiones inalámbricas NFC y Bluetooth, asegurando así que nuestra privacidad no se vea comprometida, mientras hacemos uso de ellas a través de nuestros dispositivos.

USANDO BLUETOOTH Y NFC DE FORMA SEGURA

Tanto el Bluetooth, que lleva mucho tiempo entre nosotros, como el NFC, que se ha hecho un hueco en los últimos años, son dos tecnologías que nos aportan multitud de beneficios, pero debemos asegurarnos que hacemos uso de ellas de forma segura para evitar que nuestra privacidad se vea comprometida.

1. Mantener los dispositivos actualizados.

Como hemos visto dentro de los riesgos, los ciberdelincuentes se sirven de vulnerabilidades existentes, por lo que es imprescindible mantener los dispositivos y aplicaciones actualizadas en todo momento.

Bluetooth

2. Apagar el Bluetooth cuando no lo usemos.

La manera más eficaz de evitar algún tipo de riesgo relacionado con el Bluetooth es desactivándolo. Aunque por razones obvias esto no es siempre posible, sí que es recomendable que si no estamos haciendo uso del mismo, lo mantengamos desactivado para evitar cualquier ataque o interceptación.

3. No aceptar envío de datos sin verificar la fuente.

Aunque suene simple, muchas veces tendemos a aceptar cualquier mensaje o archivo por simple curiosidad, sin pararnos a pensar que puede tratarse de un intento malicioso. Por tanto, es importante que sólo aceptemos envíos Bluetooth de fuentes que conozcamos y consideremos seguras.

4. Conectarnos solo a dispositivos de confianza.

Igual que en el punto anterior sobre el envío de datos, también podemos recibir peticiones de conexión, que debemos rechazar o ignorar si no conocemos exactamente de donde proceden, es decir, quién es la persona que está detrás de un dispositivo que está intentando establecer conexión con el nuestro.

NFC

1. Mantener los dispositivos y sus aplicaciones actualizados para evitar que los ciberdelincuentes las aprovechen para ejecutar acciones maliciosas.

2. Desactivar la tecnología NFC cuando no esté en uso desde los ajustes del dispositivo.

3. Habilitar la doble verificación para poder realizar pagos mediante NFC.

4. Conectar a través de esta tecnología solo dispositivos de confianza.