GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

INTECO
Instituto Nacional de Tecnologías de la Comunicación

Guía para proteger la red inalámbrica Wi-Fi de su hogar

OBSERVATORIO DE LA **SEGURIDAD** DE LA **INFORMACIÓN**

El Instituto Nacional de Tecnologías de la Comunicación (INTECO), sociedad estatal promovida por el Ministerio de Industria, Turismo y Comercio, es una plataforma para el desarrollo de la Sociedad del Conocimiento a través de proyectos del ámbito de la innovación y la tecnología.

El Observatorio de la Seguridad de la Información es un referente nacional e internacional al servicio de los ciudadanos, empresas y administraciones españolas para describir, analizar, asesorar y difundir la cultura de la seguridad y la confianza de la Sociedad de la Información.

Datos de contacto:
Instituto Nacional de Tecnologías de la Comunicación (INTECO)
Observatorio de la Seguridad de la Información
Avda. José Aguado, 41. Edificio INTECO. 24005 León
Teléfono: +(34) 987 877 189 / Email: observatorio@inteco.es
www.inteco.es

Depósito Legal: LE - 367 - 2009
Imprime: gráficas CELARAYN, s.a.

Índice

1. ¿En qué consiste una red Wi-Fi? ¿En qué caso es recomendable instalarla?

¿QUÉ ES WI-FI?

Es lo que comúnmente se conoce como red inalámbrica y permite la conexión a Internet sin cables. Es decir, la transmisión de la información se realiza por ondas, al igual que lo hace una radio o la televisión.

¿EN QUÉ CASOS ES RECOMENDABLE INSTALARLA?

La utilización de este tipo de conexión ofrece innumerables ventajas asociadas a la movilidad, y está especialmente recomendado en las siguientes situaciones:

- Cuando necesite conectarse desde distintos lugares en su domicilio, si resulta complicado instalar cables.
- Cuando la instalación de cables no pueda realizarse adecuadamente y puedan contrastar con la decoración de su domicilio.
- Cuando necesita conexión y movilidad al mismo tiempo.
- Cuando el **número de equipos** que se conectan en su domicilio sea **variable**.

En base a estas recomendaciones...

¿Está seguro de que realmente necesita Wi-Fi?

Debido a los posibles riesgos de seguridad que puede llevar consigo una red inalámbrica, se recomienda que compruebe la necesidad de disponer de este tipo de red. Si usted considera que realmente es necesario, ¡adelante! En esta guía encontrará recomendaciones para hacer un uso seguro de su red Wi-Fi.

2. ¿Cómo proteger su red Wi-Fi?

A la hora de instalar una red inalámbrica se deben tomar ciertas medidas para reducir los riesgos de un incidente de seguridad, como puede ser que personas ajenas accedan a su información privada, que la utilicen para cometer algún tipo de fraude sobre Ud. o sobre terceros – con la problemática legal que eso podría suponer –, o simplemente que terceros consuman ancho de banda, afectando al rendimiento.

Podemos disponer de redes Wi-Fi con un nivel de seguridad más que aceptable si se utilizan correctamente los medios de protección disponibles.

Recomendación de acceso

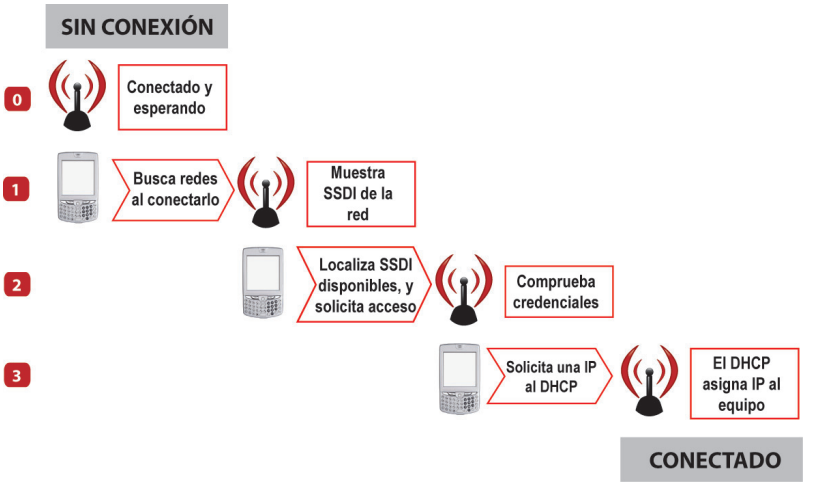
No proteger adecuadamente su red Wi-Fi puede provocar que personas ajenas la utilicen para:

1. Acceder a su información privada.
2. Cometer algún tipo de fraude, sobre Ud. o sobre terceros con la problemática legal que eso podría suponer.

Para entender mejor cómo puede asegurar su red inalámbrica, primero veremos cómo se realiza la conexión de un nuevo dispositivo a la misma.

Para asegurar la red se deberán proteger los diferentes pasos que se realizan durante la conexión del dispositivo al router.

Esquema de conexión Wi-Fi



CAMBIE LOS DATOS DE ACCESO AL *ROUTER*

El *router* que recibe cuando contrata el servicio Wi-Fi con algún proveedor, suele tener una **contraseña por defecto** para acceder a la administración y configuración del dispositivo. Esta contraseña, a veces denominada "clave del administrador", **debe cambiarse cuanto antes** por otra contraseña que sólo Ud. conozca.

No olvide cambiar la contraseña de administración de su punto de acceso inalámbrico tras su instalación.

Para mayor información sobre la creación y gestión de contraseñas puede consultar el artículo de INTECO Recomendaciones para la creación y uso de contraseñas seguras[1]. Con esta medida Ud. evitará que atacantes que hacen uso de esas contraseñas por defecto puedan tomar el control del router desde fuera vía Internet y modificar su configuración de seguridad.

OCULTE EL NOMBRE DE SU RED

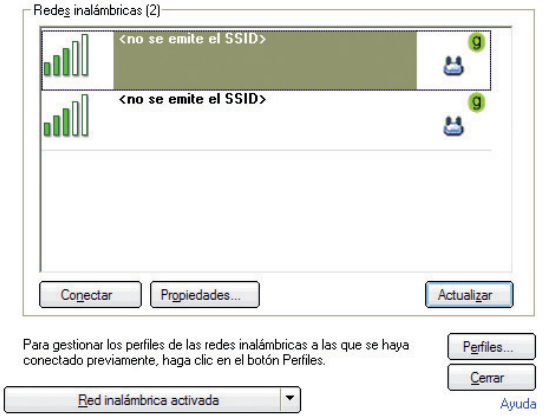
Cuando intenta conectarse a una red, le aparecerán todas las que se encuentran a su alrededor, independientemente de si le pertenecen o no, y esto mismo le ocurrirá a cualquier persona que busque las redes disponibles en la zona.

Sólo podrán conectarse a su red aquellos usuarios autorizados que conozcan el nombre de red de su empresa.

Para evitar esto, al configurar el SSID de su red en el *router*, deberá hacerlo **de forma que no se difunda el nombre de la red.** De esta manera, **si alguien quiere conectarse a ella sólo podrá hacerlo si conoce el SSID de antemano.**

1 Este documento lo puede encontrar en el siguiente link: http://www.inteco.es/Seguridad/Observatorio/Estudios_e_Informes/Notas_y_Articulos/recomendaciones_creacion_uso_contrasenas

Con esta sencilla medida se asegura el punto de la conexión, según planteábamos en el esquema de la página 7.



USE PROTOCOLOS DE SEGURIDAD

Mediante protocolos de seguridad que permiten el cifrado en función de una contraseña Ud. conseguirá proteger tanto el acceso a la red, como las comunicaciones entre dispositivos.

Utilice siempre un protocolo de seguridad y, en lo posible, el protocolo WPA.

El uso de protocolos evitará que personas no autorizadas puedan acceder a su red.

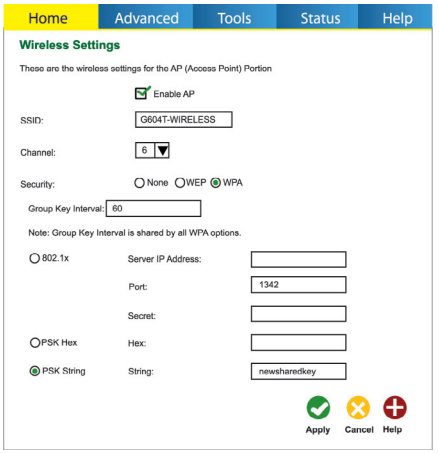
Los dos sistemas más comunes para asegurar el acceso a la red Wi-Fi son el **protocolo WEP** *(Wired Equivalent Provacy)* y el **protocolo WPA** *(WiFi Protected Access)*.

El protocolo **WEP es el más simple y lo implementan prácticamente todos los dispositivos,** pero han sido reportadas algunas vulnerabilidades que permiten saltarse su protección.

En cambio, el protocolo **WPA utiliza un cifrado más fuerte, que hace que sea más robusto,** aunque no todos los dispositivos ni sistemas operativos lo soportan (consultar documentación del dispositivo). También es posible implementar el protocolo WPA2 que es la evolución del WPA. Es el más seguro de los tres pero tampoco todos los dispositivos lo implementan.

Use el protocolo que use, la forma de trabajo es similar: si el *router* tiene habilitado el cifrado, los dispositivos receptores que traten de acceder a él tendrán que tenerlo habilitado también. Cuando el *router* detecte el intento de conexión, solicitará la contraseña que previamente habrá Ud. indicado para el cifrado.

Cómo configurar el protocolo.



Para configurar estos protocolos se recomienda consultar con el proveedor del servicio Wi-Fi o consultar el manual de router.

Para lograr una mayor seguridad se deben cambiar las contraseñas de acceso cada cierto tiempo y usar contraseñas fuertes.

Esta es una forma de asegurar el paso 2, comprobación de credenciales según el esquema de la página 7.

APAGUE EL *ROUTER* O PUNTO DE ACCESO CUANDO NO LO VAYA A UTILIZAR

De esta forma reducirá las posibilidades de éxito de un ataque contra la red inalámbrica, y por lo tanto de su uso fraudulento.

NO SE CONECTE A PUNTOS DE ACCESO NO CONOCIDOS

Hoy en día existen multitud de puntos de acceso Wi-Fi todavía sin securizar, por lo que se puede acceder a ellos fácilmente. El peligro aparece cuando se hace el propósito malicioso de engañar a los usuarios para que se conecten a ese punto de acceso.

De esta manera un usuario pensará que está usando "Internet gratis", pero lo que realmente sucede es que, al conectarse a esa red, se está permitiendo el acceso a toda la información del dispositivo a una persona no autorizada.

No crea que siempre que existen conexiones a Internet Wi-Fi gratis puede acceder "seguro" a ellas. Muchas veces es un engaño para que un desconocido pueda acceder a la información de su dispositivo.

3. Conceptos básicos de una red inalámbrica

- **SSID**
  Es el nombre de la red. Todos los paquetes de información que se envían o reciben llevan esta información.

- **WEP**
  Sistema de cifrado para redes Wi-Fi. No es seguro, ya que han aparecido vulnerabilidades que provocan que se pueda saltar fácilmente.

- **WPA**
  Sistema posterior a WEP que mejora notablemente la encriptación de WEP, aunque la versión definitiva es WPA2.

- **WPA2**
  Sistema de cifrado, evolución del WPA, con contraseña de 128 bits. Se considera seguro.

- **IP**
  Una dirección formada por una serie de números que identifica a nuestro equipo de forma unívoca dentro de una red.

- **MAC**
  Es un valor que los fabricantes asignan a cada componente de una red, y que los identifica de manera unívoca. Es como el DNI del dispositivo. Tienen dirección MAC las tarjetas de red, los routers, los USB WI-FI. En definitiva, todos los dispositivos que puedan tener una IP.

- **DHCP**
  Tecnología utilizada en redes que permite que los equipos que se conecten a una red (con DHCP activado) auto-configuren los datos de dirección IP, máscara de subred, puerta de enlace y servidores DNS, de forma que no haya que introducir estos datos manualmente.

más información

http://www.inteco.es

http://observatorio.Inteco.es

Instituto Nacional
de Tecnologías
de la Comunicación