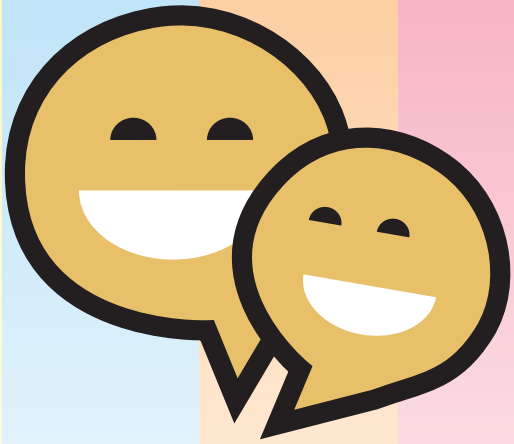
# Wi Fi

# Seguridad en redes inalámbricas



con vos en la web

www.convosenlaweb.gob.ar

PDP

Ministerio de Justicia y Derechos Humanos
Presidencia de la Nación

con vos en la web

# Seguridad en Redes inalámbricas

## ¿Qué es una red WIFI?

Es un mecanismo de conexión de dispositivos electrónicos de forma inalámbrica. Los dispositivos habilitados con WI-FI, tales como: una computadora personal, una consola de videojuegos, un teléfono inteligente, una tablet o un reproductor de audio digital, pueden conectgarse a través de un punto de acceso inalámbrica.

### Ventajas

Portabilidad: Al ser redes inalámbricas, la comodidad que ofrecen es muy superior a las redes cableadas porque cualquiera que tenga acceso a la red puede conectarse desde distintos puntos dentro de un rango, dependiendo del equipo puede variar el alcance.

Multidispositivo: Cualqueir dispositivo que tenga la tecnología WI-FI puede conectarse a los puntos de acceso. Estos puntos pueden ser públicos o privados.

### Desventajas:

La gran desventaja que poseen las redes inalámbricas es la seguridad. Una red wifi sin protección puede ser usada por terceros para acceder a Internet, a información privada o para cometer algún fraude, con las implicaciones legales que eso puede conllevar. Existen algunos programas capaces de capturar datos de las redes WI-FI en modo invasivo, de forma que pueden calcular la contraseña de la red y de esta forma acceder a ella.

## Cómo proteger la red WiFi

Para asegurar la conexión podemos implementar las siguientes medidas de fácil aplicación, simplemente con unos conocimientos básicos y la ayuda de los manuales del dispositivo.

Podemos disponer de redes WiFi con un nivel de seguridad aceptable si se utilizan correcta
mente los medios de protección disponibles

Modifica los datos por defecto de acceso al router: Los routers y puntos de acceso vienen de fabrica con contraseñas por defecto, publicamente conocidas. Cambia cuanto antes la contraseña por defecto de tu dispositivo, para evitar que atacantes puedan tomar el control del router desde el exterior.

Oculta el nombre de la red: Para evitar que un usuario con malas intenciones pueda visualizar nuestra red, es necesario configurarla para que no se difunda su nombre públicamente. De esta manera si alguien quiere conectarse a ella, solo podrá hacerlo si conoce el nombre de la red de antemano.
Para ocultar la red basta con limitar la difusión del nombre -también llamado SSID-.

con vos en la web

# Seguridad en Redes inalámbricas

Usa un protocolo de seguridad para proteger la red: Mediante protocolos de seguridad se permite el cifrado de la información en función de una contraseña. Los dos sistemas más comunes para asegurar el acceso a la red WiFi son mediante el procolo WEP y el protocolo WPA.

El mas seguro de ambos es el protocolo WPA, por lo que recomendamos su uso. También es posible utilizar el protocolo WPA2 que es la evolución del WPA, pero no todos los dispositivos lo soportan –consulta la documentación de tu dispositivo para ver si acepta WPA2 -.

Independientemente del protocolo que usemos, la forma de trabajo es similar. Si el punto de acceso o router tiene habilitado el cifrado, los dispositivos que traten de acceder a él tendrán que habilitarlo también. Cuando el punto de acceso detecte el intento de conexión, solicitará la contraseña que previamente habremos indicado para el cifrado. Utilice SIEMPRE un protocolo de seguridad, y en lo posible el protocolo WPA o WPA2

## ¿Cómo proteger la red WiFi?

Para asegurar la conexión podemos implementar las siguientes medidas de fácil aplicación, simplemente con unos conocimientos básicos y la ayuda de los manuales del dispositivo.
Podemos disponer de redes WiFi con un nivel de seguridad aceptable si se utilizan correctamente los medios de protección disponibles

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

Apagar el router o punto de acceso cuando no se vaya a utilizar: De esta forma reduciremos las probabilidades de éxito de un ataque contra la red inalámbrica y por lo tanto de su uso fraudulento.

Si cuenta con una red WI-FI en su casa u oficina recuerde siempre impedir el acceso a cualquier persona mediiante el uso de una clave que solo ustede conocerá.

**Implicancias de no hacerlo**

Económicas: el uso de su red por extraños afectará el uso de banda ancha de la conexión

Seguridad: podrían verse afectados los datos de su PC.

Judiciales: estaría facilitando los medios para realizar diversos delitos online, como la pedofilia o la piratería informática.

## Recomendaciones en el uso del celular como router WiFi

con vos en la web

# Seguridad en Redes inalámbricas

Ministerio de
Justicia y Derechos Humanos
Presidencia de la Nación

con vos en la web

buscanos también **convosenlaweb** en: twitter facebook Google+ YouTube