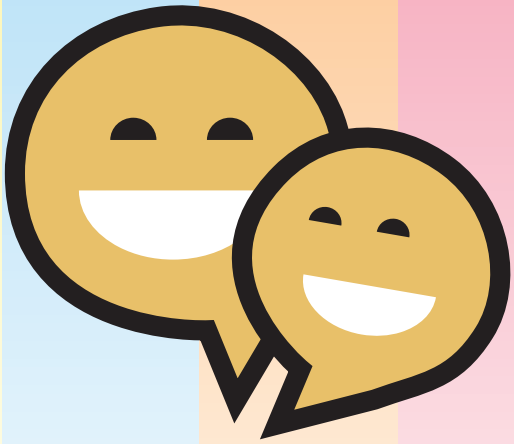
Wi Fi

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 Wi-Fi?

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 conectarse a través de un punto de acceso inalámbrico. Los smartphones también tienen la posibilidad de ser utilizados como un router Wi-Fi, al compartir la conexión 3G.

Ventajas

1. 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. Este tipo de conexión tiene distinto alcance dependiendo del equipo que se utilice.

2. Multidispositivo: Cualquier 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 Wi-Fi 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 llevar. Existen algunos programas capaces de capturar datos de las redes Wi-Fi de modo invasivo, de forma que pueden calcular la contraseña de la red y de esta forma acceder a ella. En estos casos, no sólo la conexión es más lenta sino que aquel que utiliza tu Wi-Fi tendrá acceso a la red interna y al equipo y de ese modo podrá acceder a información privada y/o confidencial. Un hacker también tendría la posibilidad de interceptar tus datos y de esta forma obtener tus contraseñas de correo electrónico, conversaciones de chat, cuentas de crédito, etc.

Cómo proteger la red Wi-Fi

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

> Es recomendable verificar bien las opciones de seguridad que brinda el router que están por instalar. Si utilizamos en forma correcta los medios de protección, tendremos una red Wi-Fi con un nivel de seguridad aceptable.

Modificá los datos por defecto de acceso al router: los routers y puntos de acceso vienen de fábrica con contraseñas por defecto, en muchos casos públicamente conocidas. Cambiá cuanto antes la contraseña por defecto de tu dispositivo, para evitar que atacantes puedan tomar el control desde el exterior y

con vos en la web

Seguridad en Redes inalámbricas

utilicen la banda ancha de tu conexión a Internet.

Ocultá 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 Service Set Identifier (SSID).

Usá un protocolo de seguridad para proteger la red: Los dos sistemas más comunes para asegurar el acceso a la red WiFi son mediante el protocolo Wired Equivalent Privacy (WEP) , el protocolo WI-Fi Protected Access (WPA) y el protocolo WP2-PSK.

El protocolo WEP fue el primer estándar de seguridad para las redes inalámbricas y su protección es muy débil, ya que sin necesidad de ser un especialista se puede romper la seguridad utilizando herramientas de hacking. En tanto, el WPA introdujo mejoras para superar las limitaciones que tenía el protocolo WEP.

El más seguro de ambos es el protocolo WPA, por lo que recomendamos su uso. También es posible utilizar el WPA2 que es la evolución del WPA. Consultá la documentación de tu dispositivo antes de comprarlo y verifica que posea este nivel de seguridad.

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. Utilizar SIEMPRE un protocolo de seguridad, y en lo posible el protocolo WPA o WPA2

Consejos prácticos de seguridad

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.

1. Contraseñas seguras: generar contraseñas seguras y cambiarlas cada cierto tiempo nos ayudarán a lograr una mayor seguridad. Evitar poner palabras obvias como “123456”, “Qwerty”, o alguna información personal como fechas de cumpleaños, aniversario, número de departamento, etc. Se recomienda combinar mayúsculas, minúsculas, números y símbolos para tener una contraseña más fuerte.

2. 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.

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

con vos en la web

Seguridad en Redes inalámbricas

Riesgos de no tomar medidas de seguridad

1. Económicas: el uso de su red por extraños afectará el uso de banda ancha de la conexión.
2. Seguridad: podrían verse afectados los datos personales de su PC
3. Judiciales: estaría facilitando los medios para realizar diversos delitos online, como la pedofilia o la piratería informática.

Recomendaciones para el uso del celular como router WiFi

Al configurar su celular como un router Wi-Fi es recomendable tomar las medidas antes mencionadas. Dependiendo el tipo de modelo y marca podremos utilizar un tipo de protección WPA o WPA2-PSK . Otra recomendación es introducir una clave de acceso para mantener la privacidad de la red Wi-Fi portátil. Es importante recordar que si el dispositivo como un punto de acceso a Internet libre, cualquier desconocido podrá utilizar la conexión 3G, teniendo los mismos beneficios y los mismos riesgos anteriormente explicados.

Ministerio de
Justicia y Derechos Humanos
Presidencia de la Nación

con vos en la web

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