

## SEGURIDAD EN REDES INALÁMBRICAS

*Si bien el creciente y constante avance evidenciado en las tecnologías de las comunicaciones permite muchas facilidades, no debemos descuidar los aspectos de seguridad que conciernen a tales progresos. El auge de las redes inalámbricas demuestra su gran versatilidad, pero muchos de quienes las utilizan a diario ignoran que sus redes están potencialmente expuestas al acceso de personas no autorizadas.*

**Autor:** Matías Ades – [arcticeye@gmail.com](mailto:arcticeye@gmail.com)

**Asesor:** Ing. Mauro Graziosi - [mgraziosi@kolossus.com.ar](mailto:mgraziosi@kolossus.com.ar)

### Introducción a las redes inalámbricas

Hace aproximadamente 20 años, para la mayoría de los usuarios las computadoras eran dispositivos independientes. A partir de los años 90 se desarrolla y se hace más utilizado el concepto de red de computadoras.

En la jerga de la informática, una **red** es un sistema de transmisión de datos que permite el intercambio de información entre ordenadores. En una red existen dos **tipos de medios de transmisión**, éstos pueden ser: *cableados* (wired) o *inalámbricos* (wireless). Dentro del primer tipo comúnmente tenemos: cable coaxial, par trenzado y fibra óptica. Por otro lado, los medios de transmisión inalámbricos usados habitualmente permiten la comunicación a través de ondas electromagnéticas, realizándose la emisión y recepción de los datos a través de antenas. También se pueden transmitir datos a cortas distancias por dispositivos que utilizan rayos infrarrojos, pero no es el foco de este artículo por sus limitaciones.

### Seguridad en redes inalámbricas

Existen dos **modos** de configurar las redes inalámbricas: *Infraestructura* o *Ad-hoc*.

El modo infraestructura es una manera de implementación en donde cada computadora se comunica con las otras siempre a través de un dispositivo administrador conocido como Access Point o Punto de Acceso (AP). Por otro lado, la modalidad Ad-hoc indica que no existe en nuestra configuración de red un nodo central o administrador (AP), sino que todos los nodos (ordenadores) están conectados directamente entre ellos.

En contraste con las redes cableadas, las redes inalámbricas tienen mucha versatilidad de conexión y de acceso. Si bien esto parece ser una ventaja por la comodidad que otorga a los usuarios, no debemos olvidar que también puede significar una facilidad para los atacantes. Es así que, por ejemplo, para conectarnos a una red cableada necesitamos tener acceso a un cable dentro del edificio, esto parece ser costoso, sumamente incómodo, y además difícil, si de hecho no tenemos autorización para hacerlo. Pero, como hemos visto, el medio de transmisión de las redes inalámbricas es, por así decirlo, el aire, y de hecho los AP pueden transmitir señales (para el envío y recepción de datos) que exceden los límites deseados. En consecuencia, cualquiera que disponga de un dispositivo portátil (notebook) con una placa de red inalámbrica y se encuentre dentro del alcance, podría tener acceso a nuestra red interna de manera casi automática.

Éste es uno de los problemas actuales que presenta esta tecnología desde el punto de vista de la seguridad. Existen soluciones de fácil implementación para evitar el acceso no autorizado a una red inalámbrica por método de autenticación.

Es así que una red inalámbrica puede clasificarse, según el método de autenticación en:

- Sin protección,
- con protección WEP, o
- WPA y WPA2

Las redes sin protección pueden ser accedidas por cualquier persona, con o sin conocimiento, con o sin intención. Sepa usted que este tipo de configuración le permite ingresar a la red simplemente con elegirla dentro del listado de redes inalámbricas disponibles dentro del alcance.

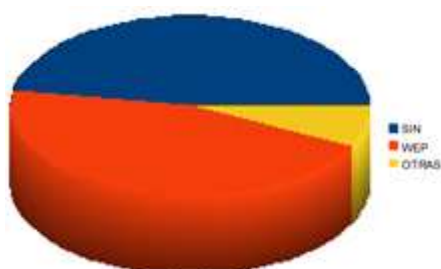
**WEP (Wired Equivalent Privacy – Privacidad Equivalente al Cableado):** Fue la primera solución en materia de seguridad que pretendía otorgar la privacidad equivalente que se tiene en redes cableadas, de allí sus siglas. Fue creado para que la información transmitida no pueda ser comprendida por cualquiera que “escuche” la red, sino únicamente por aquellos que dispongan de la clave. En realidad, si bien WEP proporciona mayor seguridad que nada, se recomienda no utilizar esta tecnología en la actualidad ya que se considera totalmente insegura desde el año 2004, inclusive para uso hogareño. En un par de minutos, alguna persona con conocimientos medios en redes inalámbricas puede acceder a su red.

**WPA (Wifi Protected Access – Acceso Protegido Wifi):** Se crea a causa de las deficiencias encontradas en el protocolo WEP. Este método incluye nuevas funciones de seguridad, lo cual hace que sea más difícil de burlar. A la hora de proteger una red, se puede aumentar la seguridad considerablemente con el solo hecho de elegir protección WPA en vez de WEP.

**WPA2:** Cumple con todos los requisitos estándares de seguridad inalámbrica y proporciona mayor seguridad que WPA, por lo que sería la elección correcta. WPA se utiliza cuando el AP no soporta WPA2 por ser un equipo viejo. WPA2 es el recomendado actualmente.

### Análisis de la situación actual

La finalidad del estudio es dar conocimiento sobre la situación de la seguridad de las redes inalámbricas instaladas en la ciudad de San Francisco, Córdoba, Argentina.



Los resultados del análisis de las redes inalámbricas en los barrios indicados fueron los siguientes:

Barrios	Tipo de Protección		
	Desprotegidas	WEP	OTRAS
2 Hermanos	2	2	2
9 de Julio	30	37	8
20 de Junio	3	5	0
25 de Mayo	59	47	5
Catedral	36	43	6
Consolata	21	25	5
Cotollengo	9	11	1
Florida	5	2	0
Güemes	2	3	0
Hospital	5	4	0
Independencia	18	16	4
Iturraspe	22	14	3
José Hernandez	13	11	2
La Milka	3	2	1
Maipú	1	2	0
Parque Industrial	11	13	2
Prado	4	5	0
Roca	68	60	10
Saenz Peña	7	6	0
Sarmiento	7	10	3
Gral. Savio	1	2	0
Velez Sarsfield	25	18	2
TOTAL	352	338	54

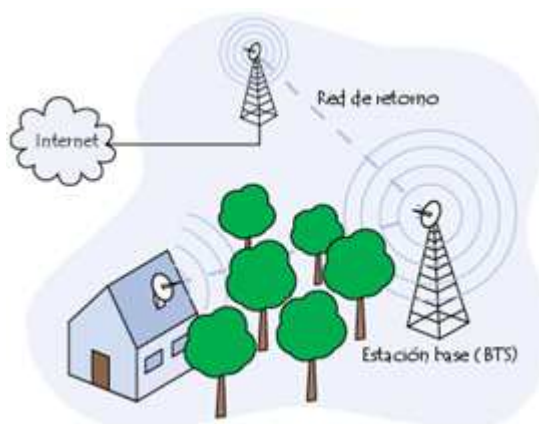
Casi la mitad de las redes inalámbricas de la ciudad de San Francisco se encuentran totalmente desprotegidas, pudiendo ser accedidas por cualquier persona sin conocimientos en redes, inclusive sin la intención de hacerlo; un poco menos de la mitad poseen protección WEP, obsoleta desde 2004, y sólo un 7% de ellas están aseguradas apropiadamente con WPA o WPA2.

Desprotegidas	WEP	OTRAS
47,31%	45,43%	7,26%

Así, puede concluirse que sólo un 7% de las redes inalámbricas de la ciudad disponen de las medidas mínimas de seguridad para hacer frente a las amenazas que atentan contra la confidencialidad de la información.

### Internet inalámbrica

Las empresas que venden Internet son conocidas como ISP (Internet Service Provider), en general brindan el servicio de acceso a Internet inalámbrico mediante la instalación de **estaciones base** o antenas de distribución. Este tipo de enlace conecta en forma conjunta a todos los usuarios de una ciudad o un área extensa.



Hay dos problemas de seguridad con algunos de los proveedores locales, el primero es que todos los usuarios que pagan por el servicio pueden acceder a las computadoras de los demás clientes del proveedor (pueden ver los recursos del otro equipo si los tienen compartidos inclusive); pero peor aún

es que un usuario que no pague por dicho servicio se puede conectar a ésta sin mayores esfuerzos, dicha acción permite al intruso tener acceso a cualquiera de los ordenadores conectados a la red.

### Para tener en cuenta...

Disponibilidad de las redes inalámbricas: sepa usted que las redes inalámbricas trabajan en frecuencias de radio que pueden coincidir con otros dispositivos, los casos más comunes son los hornos microondas y los teléfonos fijos inalámbricos. Así que en caso de que se utilicen estos dispositivos cerca de una red inalámbrica es bastante probable que esta deje de funcionar temporalmente.

Confidencialidad: lo que se quiso destacar en este artículo es que personas inexpertas o con pocos conocimientos pueden acceder al 93% de las redes de San Francisco y disponer (visualizar y/ modificar) de todos los recursos informáticos de la misma.

### Propuestas de mejora

En primera instancia, se debería evaluar si verdaderamente es necesario que la comunicación sea inalámbrica, vistos ya los riesgos que ésto implica. Por ello, tal vez pueda usarse una red cableada que es más segura y más rápida.

Si se opta por una solución inalámbrica, no utilizar ésta tecnología en modo abierto o con WEP. Se aconseja reemplazar estas implementaciones lo antes posible por WPA/WPA2 lo que implica un simple cambio en la configuración de la red. Como medida a largo plazo, se deberán revisar las implementaciones realizadas y pensar en montar otros esquemas de seguridad existentes sobre esas tecnologías (servidores VPN o servidores Radius).

Matías Ades – [arcticeye@gmail.com](mailto:arcticeye@gmail.com) (Autor)

Ing. Mauro Graziosi - [mgraziosi@kolossus.com.ar](mailto:mgraziosi@kolossus.com.ar) (Asesor)