



Las redes inalámbricas

Una mirada a su importancia y desafíos

Wireless networks. A look at their importance and challenges

Por Andric Javier Rodríguez

Resumen: Las redes inalámbricas son fundamentales en nuestra sociedad, pero ¿cuáles son las brechas de seguridad en esta tecnología? Esto lo explicamos en el presente artículo al discernir buenas prácticas para salvaguardar estas redes y el entorno de sus usuarios.

Palabras clave: Wi-Fi, punto de acceso, internet de las cosas, seguridad.

Abstract: Wireless networks are fundamental in our society, but what are the security gaps in this technology? We explain this in this article by discerning good practices to safeguard these networks and their users' environment.

Keywords: Wi-Fi, access point, internet of things, security.

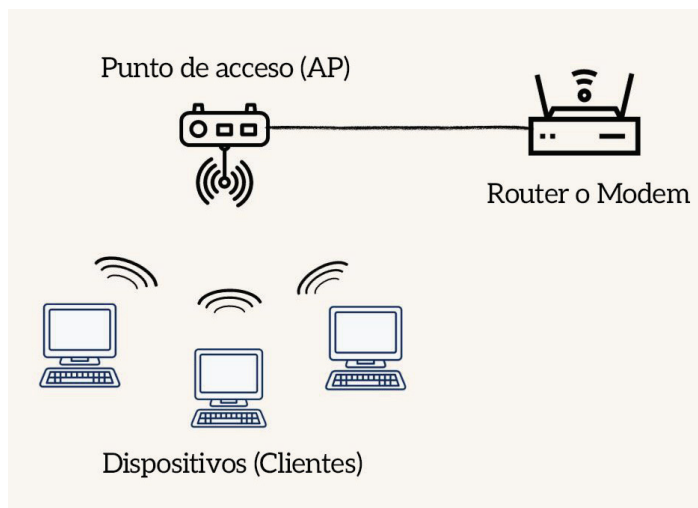
Las redes inalámbricas desempeñan un papel crucial en nuestras vidas, pues facilitan la transferencia de datos entre una multitud de dispositivos, como celulares, tabletas, relojes inteligentes y más. Estas tecnologías han redefinido nuestra forma de interactuar con la información. No solo han eliminado la necesidad de cables, sino que también han mejorado la calidad de vida de millones de personas.

En el ámbito empresarial, la gestión de redes ha ganado relevancia porque se comparten recursos e información entre los miembros de una organización. Sin embargo, este progreso no está exento de desafíos, especialmente en términos de seguridad, costo y confiabilidad (Tanenbaum y Wetherall, 2012).

Para comprender los riesgos y brechas de seguridad asociados con estas tecnologías, es esencial explorar su funcionamiento. Por ejemplo, las redes inalámbricas de com-

putadoras emplean tecnología de radiofrecuencia y el protocolo Wi-Fi para la comunicación. Los dispositivos se conectan a un punto de acceso (Access Point-AP) que, a su vez, está vinculado a un *router* para la transmisión de datos a través de señales de radiofrecuencia (Tanenbaum y Wetherall, 2012).

Figura 1. Representación del funcionamiento de un AP



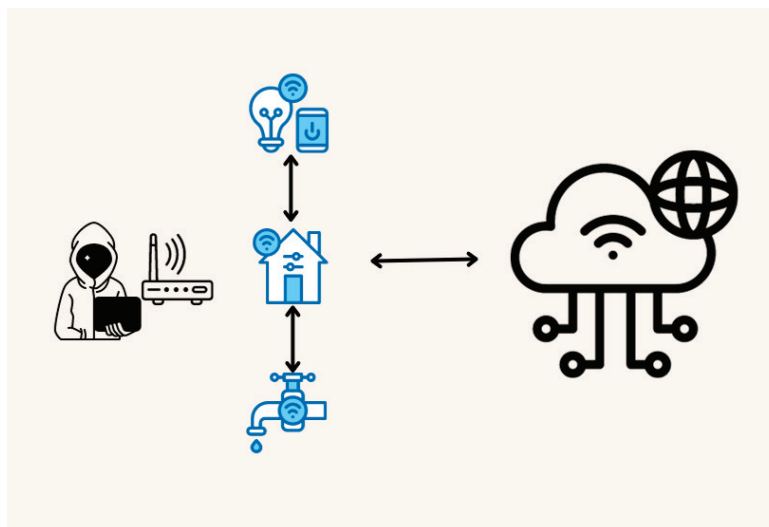
LAS REDES INALÁMBRICAS NO SOLO HAN ELIMINADO CABLES, TAMBIÉN HAN MEJORADO LA VIDA DE MILLONES DE PERSONAS

El aspecto preocupante de estas tecnologías radica en su vulnerabilidad a herramientas como *sniffers* (rastreadores), utilizadas tanto con fines éticos como maliciosos. Estos instrumentos evalúan el tráfico de la red y permiten ver todas las aplicaciones y paquetes de datos. Desafortunadamente, esta accesibilidad también permite el uso malintencionado y lleva a situaciones peligrosas como hackeos y baja confianza en la comunicación (Xia et al., 2022).

Aunque los protocolos de seguridad, como WPA2 en el caso de Wi-Fi, ofrecen cierta protección, no son infalibles. Los *sniffers* pueden sortear estas medidas con ataques de fuerza bruta, revelando las limitaciones de la seguridad inalámbrica. Esta vulnerabilidad se amplifica en dispositivos IoT (Internet of Things/internet de las cosas/), como asistentes virtuales, cámaras de seguridad y televisores inteligentes, que a menudo carecen de seguridad adecuada.

Un muestreo de 32 dispositivos IoT arrojó que 28% de estos carecía de seguridad mínima y, por tanto, expuso información sensible. Datos como dirección MAC, nombre de usuario, IP pública y más fueron transmitidos sin cifrar, lo que presenta un riesgo significativo para la privacidad de los usuarios (Wu et al., 2021).

Figura 2. Representación simple del robo de datos mediante rastreadores



La seguridad de estas redes se vuelve aún más crucial al considerar el auge de dispositivos IoT y la falta de protección en muchos de ellos. Los usuarios pueden tomar medidas para cuidar su información y aquí presentamos una lista de buenas prácticas:

- **Actualizaciones de seguridad:** Mantener actualizados los dispositivos y aplicaciones ayuda a instalar soluciones a fallos de seguridad.
- **Contraseñas robustas:** Establecer contraseñas complejas, optar por combinaciones que incluyan mayúsculas, minúsculas, caracteres y números. Ejemplo: 3spERanZ@4.
- **Desactivar conexiones inalámbricas:** Apagar Bluetooth y cerrar conexiones después de su uso previene accesos no autorizados, reduce el riesgo de intrusiones y protege la privacidad.
- **Antivirus:** Mantener activo y actualizado el antivirus ofrece otra capa de protección para la red. Algunas opciones de gratuitas son Avast y Windows Defender.



Tecnología

Foto: freepik.es /Intervención: Gerardo Mercado



EL ASPECTO
PREOCUPANTE DE
ESTAS TECNOLOGÍAS
RADICA EN SU
VULNERABILIDAD A
LOS RASTREADORES
QUE SUELEN UTILIZAR
LOS HACKERS

Estos consejos son fundamentales, y muy útiles si no somos expertos en tecnología. Aparte, en el ámbito de la ciberseguridad, se están explorando innovadores enfoques, como el uso de inteligencia artificial y métodos estadísticos para detectar anomalías en el tráfico de red de manera certera.

En conclusión, la seguridad de las redes inalámbricas es primordial en todos los entornos. Desde grandes corporativos hasta pequeños hogares, la implementación de medidas de seguridad adecuadas es esencial en esta era tecnológica. La información, en manos correctas o incorrectas, sigue siendo un poderoso activo, por ello la importancia de salvaguardarla en todo momento. 

Referencias

- Tanenbaum, Andrew. S y David J. Wetherall (2012). *Redes de Computadoras*. Pearson Education.
- Wu, Tina, Frank Breiting y Stephen Niemann (2021). "IoT network traffic analysis: Opportunities and challenges for forensic investigators?", en *Forensic Science International*, vol. 38.
- Xia, Na et al. (2022). "Optimization algorithms in wireless monitoring networks: A survey". *Neurocomputing*, vol. 489, 584-598.



Andric Rodríguez Gutiérrez es estudiante en el Centro Universitario UAEM Valle de México, de la carrera de Informática Administrativa. Poeta de usos nocturnos, amante de la luna y de la automatización mediante la informática.