Compás
capacitación e investigación
2025

Conectividad Sin Límites: Redes Inalámbricas en la Era Digital

Tecnologías, Desafíos y Aplicaciones

Oscar Cárdenas Villavicencio
Mariuxi Zea Ordóñez
Freddy Jumbo Castillo

Conectividad Sin Límites: Redes Inalámbricas en la Era Digital

Oscar Cárdenas Villavicencio
Mariuxi Zea Ordóñez
Freddy Jumbo Castillo

ISBN: 978-9942-33-994-2 DOI: http://doi.org/10.48190/9789942339942

Guayaqui, Ecuador
www.grupocompas.com
http://repositorio.grupocompas.com

Primera edición, 2025

ISBN: 978-9942-33-994-2
DOI: http://doi.org/10.48190/9789942339942
Distribución online
Acceso abierto

Primera edición 29/10/2025

Cita
Cárdenas, O., Zea, M., Jumbo, F. (2025) Conectividad Sin Límites: Redes Inalámbricas en la Era Digital. Tecnologías, Desafíos y Aplicaciones Editorial Grupo Compás

ÍNDICE DE IMÁGENES

ÍNDICE DE TABLAS

RESEÑA DEL AUTOR

Oscar Cárdenas Villavicencio, ORCID: 0000-0001-6570-8040. Correo: oecardenas@utmachala.edu.ec. Filial: Universidad Técnica de Machala. Ingeniero de Sistemas, Magíster en Telecomunicaciones y Magister en Ciencias de Datos Aplicadas, desempeña su rol como docente en la Carrera de Tecnologías de la Información en la Universidad Técnica de Machala. Su dedicación se refleja en su papel como Director del Proyecto de Vinculación SIMMO, Miembro del grupo de Investigación GIIS y en su responsabilidad como líder del Colectivo de Prácticas Laborales de la mencionada carrera, contribuyendo así al desarrollo académico y profesional de los estudiantes.

Mariuxi Zea Ordóñez, ORCID: 0000-0001-8860-6282. Correo: mzea@utmachala.edu.ec. Filial: Universidad Técnica de Machala. Ingeniera en Computación y Ciencias de la Informática con una destacada formación académica que incluye una Maestría en Sistemas de Información Gerencial y otra en Docencia Universitaria. Su experiencia se complementa con diplomados en Investigación para las Ciencias Sociales, Nuevos Paradigmas para la Docencia Superior y Docencia Superior, evidenciando su compromiso con la excelencia en la educación y la aplicación de la tecnología en el ámbito informático.

Freddy Jumbo Castillo, ORCID: 0000-0002-5200-7162. Correo: fjumbo@utmachala.edu.ec. Filial: Universidad Técnica de Machala. Ingeniero en Sistemas, Máster Universitario en Inteligencia Artificial, Master of Science y Magíster en Educación Superior, se desempeña como docente de la Carrera de Tecnologías de la Información en la Universidad Técnica de Machala. A lo largo de su trayectoria, ha participado en diversos proyectos de investigación y vinculación, enfocándose en la aplicación de soluciones tecnológicas innovadoras y la formación de profesionales con un alto sentido ético y compromiso social. Su sólida formación académica, combinada con su experiencia en el ámbito universitario, le permite contribuir de manera significativa al desarrollo y fortalecimiento tecnológico y educativo.

PREFACIO

En un mundo donde la conexión está al alcance de la mano, las redes inalámbricas se han convertido en la columna vertebral de las comunicaciones modernas. Las redes inalámbricas están en todas partes, desde la comodidad de nuestros hogares hasta la expansión del Internet de las cosas (IoT) en las ciudades.

Este libro es diseñado para brindar a los lectores una comprensión más profunda de los principios, tecnologías y desafíos detrás de esta infraestructura invisible pero esencial, donde las redes inalámbricas han evolucionado rápidamente desde los primeros días de las comunicaciones por radio hasta las redes Wi-Fi de alta velocidad y las redes móviles de próxima generación.

En cada capítulo, exploraremos los hitos clave de este desarrollo, además de observar cómo estas tecnologías están cambiando la forma en que vivimos, trabajamos y nos comunicamos, es necesario indicar que se desglosará los conceptos fundamentales detrás de las redes inalámbricas, desde la modulación de señales hasta la multiplexación y la seguridad, y se reconocerá cómo las antenas y las ondas electromagnéticas son la base de la conectividad inalámbrica y cómo la planificación de la red es esencial para un rendimiento óptimo.

OBJETIVO GENERAL DEL LIBRO

El **objetivo** principal de este libro sobre redes inalámbricas es proporcionar a los lectores una comprensión profunda y accesible de las tecnologías, conceptos y desafíos que subyacen en el mundo de la conectividad inalámbrica.

El libro está dirigido a estudiantes, profesionales e investigadores interesados en el campo de las redes inalámbricas, así como a cualquier persona que quiera ampliar sus conocimientos sobre este tema.

ESTRUCTURA DEL LIBRO

Capítulo 1: Introducción a las Redes Inalámbricas

- Definición y características.
- Historia y evolución de las redes inalámbricas.
- Tipos de redes inalámbricas: PAN, LAN, MAN, WAN.
- Ventajas y desventajas frente a las redes cableadas.
- Aplicaciones principales.
- Caso de estudio.
- Resumen Ejecutivo del Capítulo.
- Evaluación del capítulo.

Capítulo 2: Principios Básicos de las Redes Inalámbricas.

- Fundamentos de comunicación inalámbrica.

- Bandas de frecuencia y espectro radioeléctrico.
- Modulación y codificación.
- Propagación de ondas: obstáculos e interferencias.
- Componentes básicos.
- Caso de estudio.
- Resumen Ejecutivo del Capítulo.
- Evaluación del capítulo.

Capítulo 3: Estándares y Protocolos.

- IEEE 802.11: Wi-Fi.
- Bluetooth.
- Zigbee.
- LTE/5G para redes móviles.
- Comparativa entre estándares.
- Certificaciones y organismos reguladores.
- Caso de estudio.
- Resumen Ejecutivo del Capítulo.
- Evaluación del capítulo.

Capítulo 4: Consideraciones para el Diseño e Implementación de Redes Inalámbricas.

- Aspectos relevantes para el diseño de redes inalámbricas: cobertura, capacidad y seguridad
- Herramientas de análisis y planificación.
- Beneficios del uso de herramientas de análisis y planificación.
- Sugerencias para la configuración de puntos de acceso y routers inalámbricos.
- Sugerencias para la instalación y pruebas de funcionamiento.
- Solución de problemas comunes.
- Caso de estudio.
- Resumen Ejecutivo del Capítulo.
- Evaluación del capítulo.

Capítulo 5: Seguridad en Redes Inalámbricas.

- Principales amenazas y vulnerabilidades.
- Protocolos de seguridad: WEP, WPA, WPA2, WPA3.
- Autenticación y cifrado.
- Medidas para la configuración de redes seguras.
- Políticas y mejores prácticas de seguridad.
- Caso de estudio.
- Resumen Ejecutivo del Capítulo.
- Evaluación del Capítulo.

Capítulo 6: Tecnologías Emergentes.

- Wi-Fi 6 y Wi-Fi 7.
- Redes Mesh y su aplicación.

- Internet de las Cosas (IoT) y las redes inalámbricas.
- Tendencias futuras.
- Caso de estudio.
- Resumen Ejecutivo del Capítulo.
- Evaluación del capítulo.

Capítulo 7: Regulaciones y Normativa.

- Implicaciones Legales de la Seguridad Inalámbrica
- Regulaciones Internacionales sobre Seguridad Inalámbrica.
- Desafíos Legales en la Seguridad de Redes Inalámbricas.
- Responsabilidades de Empresas y Usuarios.
- Regulación y Normativas en el Ecuador.
- Desafíos de la Regulación en Ecuador.
- Perspectivas Futuras en la Regulación.
- Caso de estudio.
- Resumen Ejecutivo del Capítulo.
- Evaluación del capítulo.

CARACTERÍSTICAS PEDAGÓGICAS

- **Casos de Estudio:**
  Se incluirán casos de estudio para aplicar los conocimientos adquiridos.
- **Preguntas de Repaso**
  Preguntas de repaso al final de cada capítulo para consolidar la comprensión.

EJERCICIO DE INTRODUCCIÓN A LAS REDES INALÁMBRICAS

Descubre tu Señal Wi-Fi

Objetivo: Familiarizarse con los conceptos de señal Wi-Fi y fortaleza de la señal.

Este sencillo ejercicio permite a los lectores experimentar cómo cambia la intensidad de la señal Wi-Fi según su posición relativa al enrutador, además ayuda a comprender la importancia de la ubicación estratégica de los equipos de red inalámbrica y como la interferencia afecta la calidad de la conexión.

Instrucciones:

a. En casa o en la oficina, lleva un dispositivo (teléfono, portátil o tableta) conectado a tu red Wi-Fi.
b. Encuentre una ubicación central en la misma habitación que su enrutador o punto de acceso Wi-Fi.
c. Observe la intensidad de la señal de Wi-Fi en el dispositivo. Generalmente aparece como una barra o un número en la configuración de Wi-Fi de su dispositivo. Tómese el tiempo para comprender cómo se muestra la intensidad de la señal en su dispositivo.
d. Ahora comience a moverse lentamente por la habitación hasta una esquina o área alejada del enrutador Wi-Fi.
e. Observe cómo cambia la intensidad de la señal de Wi-Fi a medida que se aleja del enrutador, y observe las barras o números que indican la intensidad de la señal.
f. Registre sus observaciones y considere las siguientes preguntas**: ¿Cuál es la intensidad de la señal en diferentes partes de la habitación? ¿Qué factores afectan la intensidad de la señal, como la interferencia de paredes u otros dispositivos?**
g. Comparta sus resultados con otras personas en casa o en la oficina y compare los resultados.

Capítulo1: Introducción a las Redes Inalámbricas

Las redes inalámbricas representan una tecnología esencial en la comunicación moderna, caracterizada por la ausencia de cables físicos para la transmisión de datos. Estas tecnologías se basan en el uso de ondas electromagnéticas para conectar dispositivos, brindando mayor flexibilidad y movilidad en entornos personales, profesionales e industriales. La expansión de estas redes ha transformado significativamente cómo interactuamos con la tecnología, permitiendo el acceso instantáneo a información y servicios desde cualquier lugar y en cualquier momento. En este capítulo se exploran los conceptos básicos de las redes inalámbricas, su historia, clasificación, ventajas y desventajas comparativas con las redes cableadas y además se abordan las aplicaciones clave, destacando su papel en la transformación digital de la sociedad (Kurose y Ross, 2021).

Objetivos del Capítulo:

- Definir con precisión el concepto de redes inalámbricas, reconociendo sus características técnicas fundamentales y su funcionamiento general en comparación con otras tecnologías de red.
- Describir la evolución histórica de las redes inalámbricas, identificando los hitos tecnológicos más relevantes y su impacto en el desarrollo de las comunicaciones móviles y digitales.
- Distinguir los principales tipos de redes inalámbricas –WPAN, WLAN, WMAN y WWAN– considerando su arquitectura, alcance, tecnologías utilizadas y ejemplos de aplicación en la vida real.
- Comparar las ventajas y limitaciones de las redes inalámbricas frente a las redes cableadas, evaluando criterios como flexibilidad, seguridad, velocidad, costos y facilidad de implementación en distintos entornos.
- Analizar casos de uso y aplicaciones prácticas de las redes inalámbricas, con énfasis en los sectores residencial, empresarial, educativo, industrial y de salud, destacando su relevancia en la transformación digital contemporánea.

1.1. Definición y características

Las redes inalámbricas son sistemas que permiten la comunicación de datos sin el uso de cables físicos, utilizando en su lugar ondas electromagnéticas como medio de transmisión.

Imagen 1: Características de las redes inalámbricas
Fuente: Elaboración propia.

Las redes son esenciales en la conectividad moderna debido a las siguientes características:

- **Movilidad**: Proporcionan acceso a la red desde cualquier lugar dentro del área de cobertura, facilitando el trabajo remoto y la movilidad, para que los usuarios pueden conectarse desde diversos dispositivos, como computadoras portátiles, smartphones y tabletas (Tanenbaum et al., 2021).
- **Flexibilidad**: Permiten una rápida instalación y configuración, especialmente en lugares donde el cableado es impráctico, esto resulta ideal para eventos temporales o lugares con restricciones arquitectónicas.
- **Escalabilidad**: Facilitan la ampliación de la red para incluir más dispositivos sin cambios significativos en la infraestructura, esto es especialmente útil en entornos empresariales y educativos.
- **Interoperabilidad**: Soportan diferentes dispositivos y plataformas, promoviendo la conectividad universal (Kurose y Ross, 2021).
- **Costos operativos**: En ciertas situaciones, los costos asociados a las redes inalámbricas pueden ser más bajos que los de las redes cableadas, especialmente en entornos donde el cableado resulta inviable.

1.2. Historia y evolución de las redes inalámbricas.

La evolución de las redes inalámbricas es el resultado de avances tecnológicos y descubrimientos científicos a lo largo de más de un siglo:

- **Finales del siglo XIX**: La comunicación inalámbrica comenzó con la invención de la radio por Guglielmo Marconi en 1895, donde permitió la transmisión de señales a larga distancia sin necesidad de cables, permitiendo establecer las bases para futuros desarrollos.
- **Años 1940-1950:** Durante la Segunda Guerra Mundial, se realizaron avances significativos en tecnologías de radar y comunicaciones por microondas, impulsados por necesidades militares.
- **Década de 1970:** La introducción de los sistemas de comunicación por satélite marcó un hito en la conectividad global, permitiendo la transmisión de datos a través de grandes distancias geográficas.
- **Década de 1980:** Se desarrollaron las primeras redes celulares analógicas (1G), que revolucionaron la comunicación personal al introducir la telefonía móvil, aunque limitadas en capacidad y velocidad, estas redes sentaron las bases para las generaciones futuras.
- **Década de 1990:** La estandarización del Wi-Fi (IEEE 802.11) en 1997 transformó la conectividad inalámbrica al proporcionar acceso rápido y confiable a internet, además durante esta época también se introdujeron las redes 2G, que ofrecieron comunicaciones digitales y servicios de datos básicos (IEEE Standards Association, 2023).
- **Años 2000:** Con la llegada de 3G, las redes inalámbricas alcanzaron una velocidad suficiente para soportar aplicaciones como la navegación web y el streaming de audio, donde además se popularizaron los dispositivos móviles como smartphones y laptops.
- **Años 2010:** Las redes 4G LTE (Long Term Evolution) ofrecieron velocidades de banda ancha comparables a las conexiones cableadas, permitiendo la proliferación de servicios como videoconferencias, juegos en línea y contenido de alta definición, en este período también vio el auge del Internet de las Cosas (IoT).
- **Actualidad:** La tecnología 5G representa la última generación de redes inalámbricas, proporcionando latencias ultrabajas, velocidades de hasta 10 Gbps y la capacidad de conectar millones de dispositivos simultáneamente. Estas capacidades han abierto nuevas

posibilidades en campos como la inteligencia artificial, la automatización industrial y la telemedicina (Bellis, 2019).

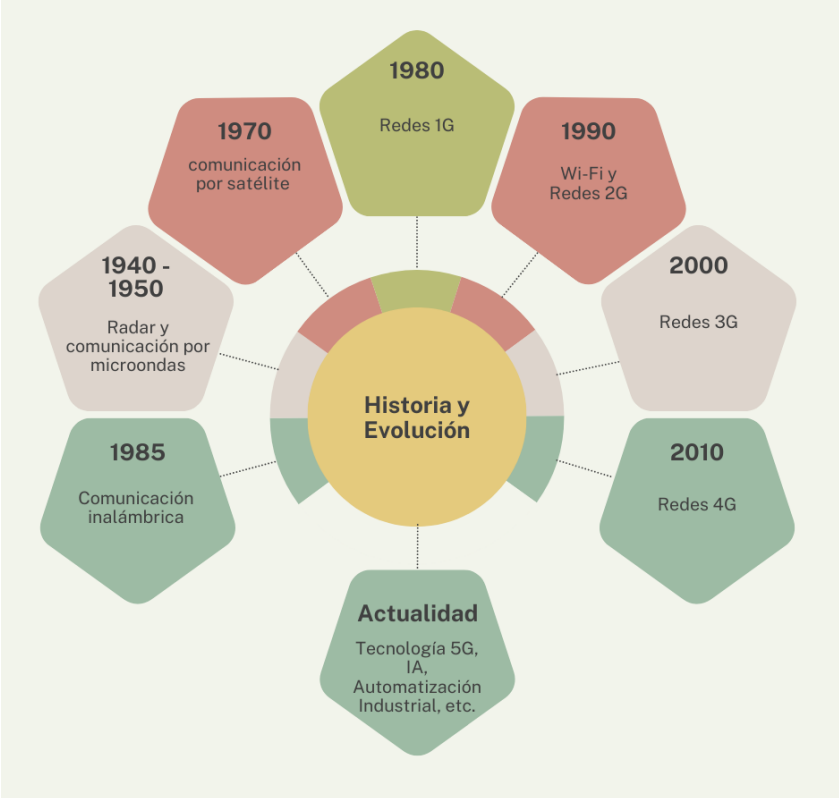

Imagen 2: Historia y Evolución de las redes Inalámbricas
Fuente: Elaboración propia.

1.3. Tipos de redes inalámbricas.

Las comunicaciones inalámbricas pueden organizarse en diversas categorías según el criterio que se utilice; en este caso específico, se agrupan según su alcance, el cual determina la distancia máxima que puede existir entre los dos extremos que intervienen en la comunicación inalámbrica y, por lo tanto, estas mismas se clasifican en distintos grupos:

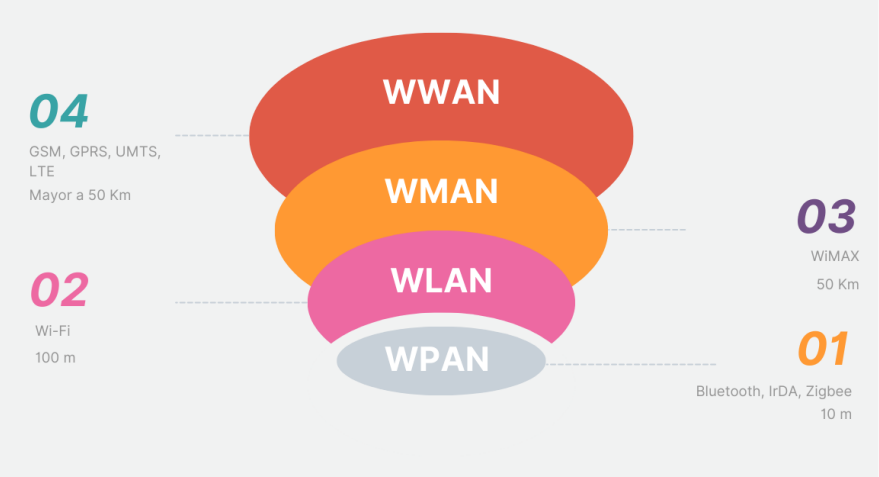

Imagen 3: Clasificación de las redes inalámbricas
Fuente: Elaboración propia.

- **Redes inalámbricas de área personal o WPAN** (Wireless Personal Area Network): Estas redes se basan en el estándar IEEE 802.15 y están diseñadas para conectar dispositivos en un rango cercano, generalmente dentro de un radio de 10 metros. Tecnologías como Bluetooth e Infrared Data Association (IrDA) son ejemplos comunes de WPAN, por lo tanto, estas redes son ideales para aplicaciones de baja potencia y sincronización de dispositivos personales, como auriculares, relojes inteligentes y dispositivos médicos portátiles (Tanenbaum et al., 2021).
- **Redes inalámbricas de área local o WLAN** (Wireless Local Area Network): Las WLAN conectan dispositivos dentro de un área limitada, como oficinas, hogares o campus, donde utilizan principalmente Wi-Fi (IEEE 802.11) para proporcionar acceso a internet y compartir recursos, como impresoras y almacenamiento en red, por otra parte, su cobertura puede variar entre 30 y 100 metros dependiendo de la infraestructura, ya que las WLAN son conocidas por su flexibilidad y facilidad de instalación (IEEE Standards Association, 2023).
- **Redes inalámbricas de área metropolitana o WMAN** (Wireless Metropolitan Area Network): Este tipo de red cubre áreas metropolitanas completas y conecta múltiples redes locales en una región urbana, como, por ejemplo, utilizan tecnologías como WiMAX (Worldwide Interoperability for Microwave Access), ofreciendo conectividad de banda ancha para servicios de gobierno, empresas y universidades, siendo una alternativa a las conexiones de fibra óptica en áreas urbanas densas (Kurose y Ross, 2021).
- **Redes inalámbricas de área extensa o WWAN** (Wireless Wide Area Network): Las WWAN son redes de mayor alcance que

abarcan áreas geográficas extensas, incluyendo países y continentes, las mismas que dependen de tecnologías celulares como 3G, 4G LTE y 5G, además de enlaces satelitales y son esenciales para la conectividad móvil global, permitiendo que dispositivos accedan a internet desde cualquier ubicación. Algunas aplicaciones comunes incluyen servicios de GPS, comunicación de emergencia y redes empresariales multinacionales (Bellis, 2019).

1.4. Ventajas y desventajas frente a las redes cableadas.

A continuación, se presenta un cuadro sobre las principales ventajas y desventajas de las redes inalámbricas frente a las cableadas:

Tabla 1: Redes Inalámbricas vs Redes Cableadas

Ventajas	Desventajas
Movilidad: permite conectarse desde cualquier lugar dentro del alcance.	**Menor velocidad:** las redes inalámbricas suelen ser más lentas que las cableadas.
Instalación rápida: no requiere de cableado físico, lo que reduce tiempo y costos.	**Mayor vulnerabilidad:** las señales inalámbricas pueden ser interceptadas fácilmente.
Escalabilidad: añadir dispositivos a la red es más sencillo y flexible.	**Interferencias:** paredes, dispositivos electrónicos y condiciones climáticas pueden afectar el rendimiento.
Menores costos iniciales: ideal para lugares temporales o de difícil acceso.	**Latencia variable:** en algunas aplicaciones críticas, puede afectar el desempeño.
Facilidad de acceso: permite la conexión de dispositivos diversos sin configuración física.	**Consumo energético:** los puntos de acceso inalámbricos necesitan alimentación constante.

Flexibilidad de ubicación: no están restringidas por la longitud de los cables.	**Seguridad limitada:** es necesario implementar medidas avanzadas como cifrado WPA3.

Fuente: Elaboración propia.

1.5. Aplicaciones principales.

Las redes inalámbricas tienen un impacto significativo en diversos sectores, permitiendo un sinfín de aplicaciones prácticas, de las cuales destacan:

- **Salud**: Las redes inalámbricas han transformado la atención médica, facilitando la telemedicina, telecuidado, el monitoreo remoto de pacientes y la integración de dispositivos médicos portátiles que miden parámetros como presión arterial, frecuencia cardíaca y niveles de glucosa, donde es necesario mencionar que estas tecnologías permiten una respuesta rápida ante emergencias y la gestión eficiente de enfermedades crónicas (Tanenbaum et al., 2021).
- **Educación:** La conectividad inalámbrica ha democratizado el acceso al conocimiento a través del aprendizaje en línea y plataformas de educación virtual, por otra parte, en las aulas se facilita el uso de dispositivos compartidos, herramientas de colaboración en tiempo real y acceso instantáneo a recursos educativos (Kurose y Ross, 2021).
- **Industria:** En el sector industrial, las redes inalámbricas soportan la automatización y monitoreo de procesos en tiempo real, como por ejemplo los sensores inalámbricos ayudan en la gestión de inventarios, el control de maquinaria y la mejora de la productividad en líneas de producción.
- **Hogares inteligentes:** Los hogares inteligentes aprovechan redes inalámbricas para conectar dispositivos como termostatos, sensores, cámaras de seguridad, luces y asistentes virtuales, mejorando la comodidad, eficiencia energética y seguridad del hogar
- **Agricultura:** En entornos rurales, las redes inalámbricas permiten el monitoreo de cultivos, riego automatizado y gestión de ganado mediante drones y sensores IoT, optimizando los recursos y mejorando los rendimientos agrícolas.

- **Transporte:** Las redes inalámbricas son fundamentales para los sistemas de transporte inteligente (ITS), que incluyen vehículos autónomos, gestión del tráfico en tiempo real y sistemas de peaje electrónico, donde dichas aplicaciones mejoran la seguridad y la eficiencia del transporte (Dirección General de Tráfico de España, 2022).

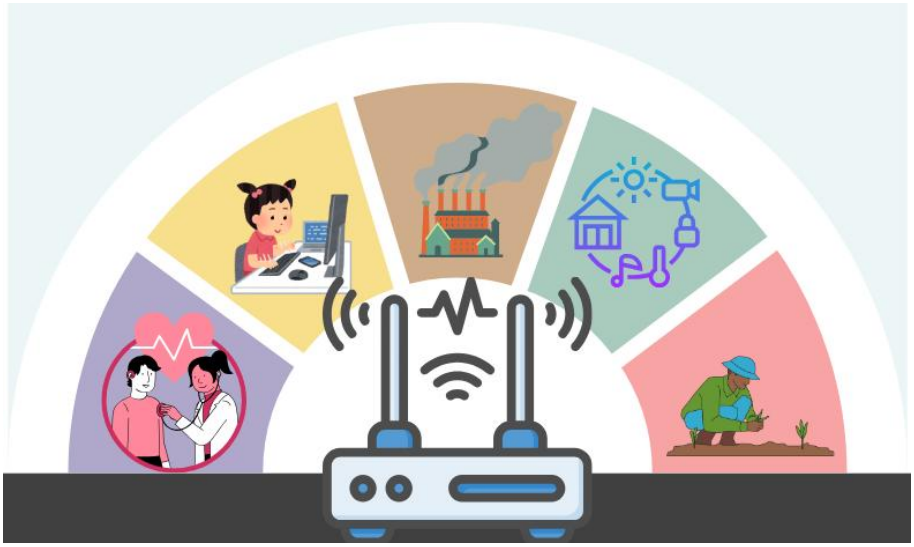

Imagen 4: Redes inalámbricas en el Sector Empresarial
Fuente: Elaboración propia.

1.6. Caso de estudio

Un hospital rural ubicado en una zona de difícil acceso no cuenta con una infraestructura adecuada de comunicación y enfrenta problemas para compartir información entre sus áreas de emergencia, consulta externa y administración. Para solucionar esta problemática, el hospital decide implementar una red inalámbrica que permita interconectar sus dispositivos médicos, mejorar la comunicación entre el personal y proporcionar acceso a internet para los pacientes y sus familiares.

Los objetivos principales de la implementación son:

- Garantizar una comunicación fluida entre las distintas áreas del hospital.
- Mejorar la eficiencia en el monitoreo remoto de pacientes.
- Optimizar el acceso a los historiales médicos electrónicos mediante una red segura y confiable.
- Ofrecer conectividad básica para pacientes y familiares.

Tras la implementación, el hospital logra mejorar sus tiempos de respuesta en emergencias y la calidad del servicio a los pacientes,

reduciendo costos en infraestructura cableada y permitiendo mayor flexibilidad en la expansión de su red en el futuro.

Preguntas de análisis:

1. ¿Cuál fue el principal problema que enfrentaba el hospital rural antes de la implementación de la red inalámbrica?
2. ¿Cómo impacta la conectividad inalámbrica en la calidad del servicio de salud en zonas rurales?
3. ¿Qué beneficios ofrece una WLAN en comparación con una red cableada en un entorno hospitalario?

1.7. Resumen Ejecutivo del Capítulo

El capítulo ofreció una visión general de las redes inalámbricas, destacando su definición como sistemas de comunicación que emplean ondas electromagnéticas en lugar de cables físicos, donde se describen sus principales características: movilidad, flexibilidad, escalabilidad e interoperabilidad. La historia de estas redes se remonta a la invención de la radio en 1895 y avanza hasta las tecnologías 5G actuales. Se clasifica a las redes inalámbricas en WPAN, WLAN, WMAN y WWAN, diferenciándose por su alcance y aplicaciones. Se comparan con las redes cableadas, resaltando ventajas como la instalación rápida y desventajas como la susceptibilidad a interferencias, además, se exploran sus aplicaciones en sectores clave como salud, educación, industria, hogares inteligentes, agricultura y transporte, por último, el capítulo concluye con un caso de estudio en un hospital rural, evidenciando cómo una red inalámbrica mejora la eficiencia y la atención médica, reforzando así la importancia de esta tecnología en la transformación digital contemporánea.

1.8. Evaluación del capítulo.

¿Cuál es una ventaja principal de las redes inalámbricas frente a las cableadas?

a) Menor costo de mantenimiento
b) Mayor estabilidad de la señal
c) Movilidad y flexibilidad
d) Mayor velocidad de transmisión

¿Cuál de las siguientes tecnologías se usa en una WPAN?

a) WiMAX
b) Bluetooth
c) 4G LTE
d) Ethernet

¿Qué estándar de redes inalámbricas es más común en las WLAN?

a) IEEE 802.11
b) IEEE 802.3
c) IEEE 802.15
d) IEEE 802.16

¿Cuál de las siguientes afirmaciones sobre las redes WMAN es correcta?

a) Son redes que conectan dispositivos en un mismo edificio.
b) Se utilizan para interconectar redes LAN en una ciudad.
c) Son utilizadas únicamente para redes móviles.
d) Funcionan con tecnología Bluetooth.

¿Cuál de las siguientes afirmaciones es una desventaja de las redes inalámbricas?

a) Permiten la movilidad del usuario.
b) Son más fáciles de instalar que las cableadas.
c) Son más susceptibles a interferencias electromagnéticas.
d) Pueden expandirse sin costos adicionales.

REFERENCIAS BIBLIOGRÁFICAS

Bellis, M. (2019). The History of Radio Technology. ThoughtCo: https://www.thoughtco.com/invention-of-radio-1992382

Dirección General de Tráfico de España. (2022). Sistemas Inteligentes de Transportes. DGT: https://www.dgt.es/muevete-con-seguridad/tecnologia-e-innovacion-en-carretera/sistemas-inteligentes-de-transporte-its/

IEEE Standards Association. (2023). Beyond Standards. IEEE SA: https://standards.ieee.org/beyond-standards/the-evolution-of-wi-fi-technology-and-standards/

Kurose, J., & Ross, K. (2021). Computer Networking: A Top-Down Approach (8 th. ed.). Pearson Education Limited. https://doi.org/978-1-292-40546-9

Tanenbaum, A., Feamster, N., & Wetherall, D. (2021). Computer Networks (Vol. 6a). Pearson Education Limited. https://doi.org/978-1292374062

Capítulo2: Principios Básicos de las Redes Inalámbricas

Las redes inalámbricas se han consolidado como una tecnología esencial en la era de la conectividad y la comunicación digital, permitiendo que sistemas complejos como el Internet de las Cosas (IoT), revolucionen la forma en que individuos y organizaciones se relacionen con el entorno digital. Este capítulo presenta los principios fundamentales que sustentan el funcionamiento de las redes inalámbricas, proporcionando un marco teórico y técnico indispensable para su comprensión integral. Entre los temas abordados se incluyen los conceptos clave de la comunicación inalámbrica, las bandas de frecuencia utilizadas, los métodos de modulación y codificación, la propagación de ondas electromagnéticas, así como los componentes esenciales que posibilitan su operación. El dominio de estos conocimientos resulta crucial para el diseño, la implementación y el mantenimiento de redes inalámbricas eficientes, seguras y adaptadas a las demandas de los entornos actuales.

Objetivos del capítulo:

- Comprender los principios fundamentales de la comunicación inalámbrica, reconociendo su importancia en el diseño, operación y expansión de redes modernas, especialmente en contextos de movilidad y acceso ubicuo.
- Identificar las bandas de frecuencia y el espectro radioeléctrico asignados para las comunicaciones inalámbricas, diferenciando sus usos según normativa internacional y las tecnologías que las emplean (Wi-Fi, Bluetooth, LTE, entre otras).
- Explicar los principios de modulación y codificación digital aplicados a la transmisión de datos por medios inalámbricos, con énfasis en cómo estos procesos optimizan la eficiencia y la confiabilidad de la señal.
- Analizar los factores físicos y ambientales que afectan la propagación de las ondas electromagnéticas, tales como la atenuación, los obstáculos estructurales, la interferencia electromagnética y la distancia.
- Describir los componentes esenciales de una red inalámbrica, incluyendo su función y configuración básica: puntos de acceso, antenas, adaptadores o tarjetas de red, y su interrelación dentro de la infraestructura de red.

2.1. Fundamentos de comunicación inalámbrica.

La comunicación inalámbrica implica la transmisión de datos a través de ondas electromagnéticas sin necesidad de cables físicos, esto se logra mediante el uso de señales de radiofrecuencia (RF) que transportan información desde un transmisor hasta un receptor, permitiendo que las

tecnologías inalámbricas evolucionen de manera significativa en los últimos años, abarcando desde redes de corto alcance como Bluetooth hasta infraestructuras globales como las redes de telecomunicaciones móviles 5G.

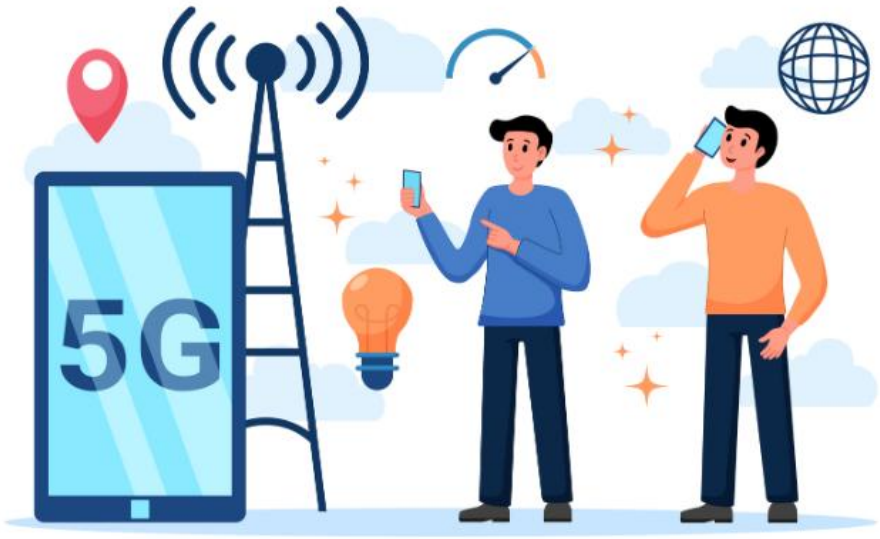

Imagen 5: Redes de telecomunicaciones móviles 5G.
Fuente: Elaboración propia.

Los sistemas de comunicación inalámbrica pueden clasificarse según su alcance y aplicación en redes de área personal (PAN), redes de área local (LAN), redes de área metropolitana (MAN) y redes de área extensa (WAN), tal como se explicó en el capítulo anterior, donde estas redes dependen de diversos estándares y protocolos para garantizar la interoperabilidad y la seguridad de la información transmitida.

Entre sus ventajas destacan la movilidad, la flexibilidad y la capacidad de implementar redes en áreas de difícil acceso como las zonas rurales, pero permiten una reducción en los costos de infraestructura en comparación con las redes cableadas; sin embargo, presentan desafíos como la interferencia de señales, la latencia en la transmisión y la vulnerabilidad a ataques de seguridad.

La expansión de las redes inalámbricas ha representado un cambio significativo en la manera en que las personas acceden a la información, eliminando las limitaciones impuestas por la infraestructura cableada y permitiendo la conectividad desde cualquier ubicación y en cualquier momento (Stallings, 2013).

2.2. Bandas de frecuencia y espectro radioeléctrico.

El espectro radioeléctrico es el rango de frecuencias de ondas electromagnéticas utilizadas para la comunicación, este recurso limitado está regulado por organismos gubernamentales y se clasifica en bandas de frecuencia específicas que se asignan para diferentes usos, como telecomunicaciones, radiodifusión y redes inalámbricas. Las principales bandas de frecuencia utilizadas en redes inalámbricas son las siguientes:

- **2.4 GHz:** Usada en redes Wi-Fi (802.11b/g/n) y Bluetooth, dicha banda ofrece una buena cobertura debido a su capacidad para atravesar paredes y obstáculos, pero sufre interferencias de otros dispositivos que operan en la misma frecuencia, como microondas y teléfonos inalámbricos, además, tiene solo 3 canales no superpuestos, lo que limita su capacidad en entornos densos.
- **5 GHz:** Utilizada en redes Wi-Fi (802.11a/n/ac/ax), esta banda proporciona mayores velocidades y menos interferencias gracias a la disponibilidad de hasta 23 canales no superpuestos; sin embargo, su alcance es menor en comparación con la banda de 2.4 GHz debido a la mayor atenuación de las señales de alta frecuencia.
- **6 GHz:** Introducida con Wi-Fi 6E, esta banda expande la capacidad de las redes inalámbricas al proporcionar 1200 MHz adicionales de espectro, donde ofrece canales más anchos (hasta 160 MHz) y menor latencia, lo que la hace ideal para aplicaciones de alta demanda como realidad virtual y streaming en 4K.
- **Sub-1 GHz (900 MHz):** Utilizada en tecnologías como Zigbee y LoRaWAN para IoT, esta banda es efectiva para aplicaciones de largo alcance y baja potencia, como sensores en entornos rurales o industriales.

Además de estas bandas específicas, el espectro radioeléctrico incluye frecuencias utilizadas por tecnologías emergentes:

- **Ondas milimétricas (mmWave):** Operan en el rango de 24 a 100 GHz y representan una innovación clave en las redes 5G al proporcionar velocidades de transmisión de datos extremadamente altas y una latencia mínima, permitiendo aplicaciones avanzadas como realidad aumentada, telemedicina y vehículos autónomos; sin embargo, estas ondas presentan desafíos significativos debido a su corta longitud de onda, lo que las hace susceptibles a la absorción por obstáculos como edificios, árboles y hasta la humedad en el aire (Rappaport et al., 2014).
- **Banda de TVWS (TV White Spaces):** Se refiere a las frecuencias del espectro radioeléctrico que no están en uso por servicios de

radiodifusión de televisión en ciertas áreas geográficas, pero dichas frecuencias pueden ser aprovechadas para proporcionar conectividad inalámbrica en zonas rurales y de difícil acceso, ofreciendo una alternativa eficiente para reducir la brecha digital. El uso del espectro de TVWS facilita la expansión de la conectividad en áreas remotas, gracias a una infraestructura asequible y una mejor propagación de la señal en comparación con las bandas convencionales de Wi-Fi.

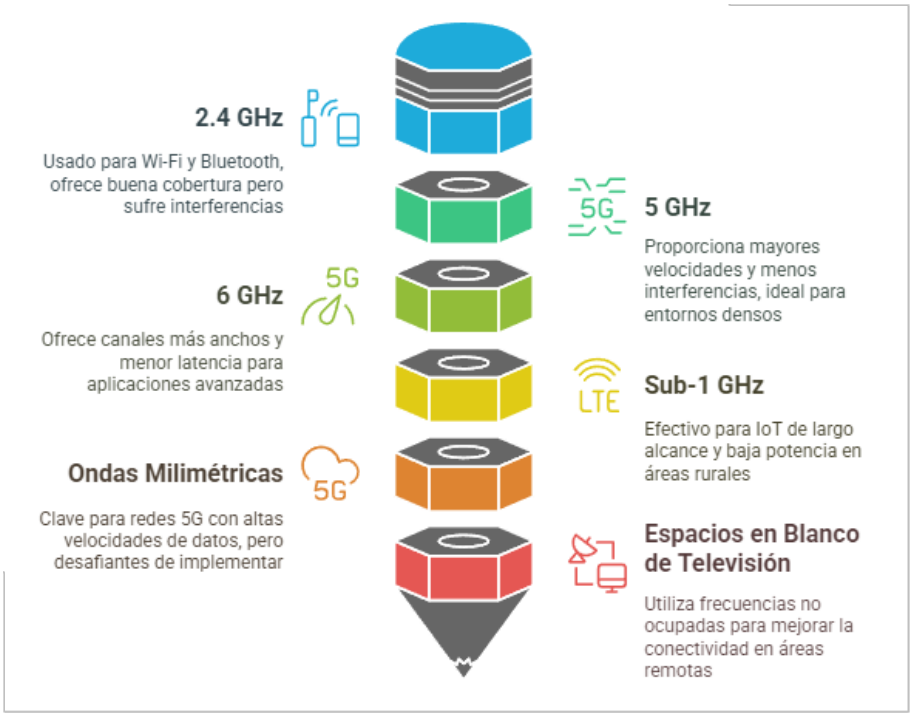

Imagen 6: Comprendiendo el espectro radioeléctrico.
Fuente: Elaboración propia.

Regulación del espectro

El espectro radioeléctrico está regulado por entidades como la Unión Internacional de Telecomunicaciones (UIT) y autoridades locales como la FCC en Estados Unidos, estas organizaciones asignan bandas de frecuencia para evitar interferencias y maximizar su uso, por ejemplo, en redes Wi-Fi, las bandas de 2.4 GHz y 5 GHz son de uso libre bajo ciertas restricciones de potencia, donde dicho tema se lo tratará más a fondo en los siguientes capítulos.

2.3. Modulación y codificación.

La modulación es el proceso mediante el cual una señal portadora es alterada para transportar información de manera eficiente a través de un canal de comunicación inalámbrico, siendo fundamental en las redes inalámbricas modernas, ya que permite la optimización del ancho de

banda y la reducción de interferencias, donde las técnicas de modulación no solo posibilitan la transmisión de datos, sino que también optimizan el uso del espectro y aumentan la resistencia a las interferencias y el ruido. (Proakis y Salehi, 2007).

Por otro lado, la codificación es el proceso de conversión de los datos en una forma estructurada antes de la transmisión, lo que permite la detección y corrección de errores para garantizar una comunicación confiable, dicho proceso es esencial en sistemas inalámbricos debido a la presencia de ruido, interferencias y pérdidas de señal. Existen dos principales tipos de codificación:

Codificación de fuente: Reduce la redundancia de los datos antes de la transmisión, mejorando la eficiencia del ancho de banda, donde se incluyen la compresión Huffman y la codificación aritmética.

Codificación de canal: Introduce redundancia controlada en los datos para detectar y corregir errores, entre estos métodos comunes se incluyen:

- **Códigos de bloque:** Como los códigos de Hamming y Reed-Solomon, utilizados en redes Wi-Fi y en discos ópticos.
- **Códigos convolucionales:** Aplicados en sistemas de telecomunicaciones como LTE y 5G, donde permiten la corrección de errores en tiempo real.
- **Turbo códigos y códigos LDPC (Low-Density Parity-Check):** Son los más avanzados y utilizados en redes de alta capacidad como 5G y satélites (Molisch, 2022).

La combinación de técnicas de modulación y codificación mejora significativamente la eficiencia y confiabilidad de las redes inalámbricas, permitiendo la transmisión de datos en entornos hostiles y con limitaciones de ancho de banda. Los métodos principales de modulación incluyen:

- **ASK (Keying de Amplitud):** En este esquema, la amplitud de la onda portadora varía de acuerdo con los datos binarios transmitidos, aunque es sencillo y de fácil implementación, es altamente susceptible a interferencias y variaciones en la potencia de la señal, lo que lo hace menos eficiente en entornos con alto nivel de ruido (Proakis y Salehi, 2007).
- **FSK (Keying de Frecuencia):** Cambia la frecuencia de la onda portadora dependiendo del valor binario (0 o 1), este método es más resistente al ruido que ASK y se emplea en sistemas de baja velocidad como pagers y redes de

telemetría. Es necesario mencionar que esta técnica se aplica en entornos donde la estabilidad de la señal y la velocidad de transmisión son variables que se tienen que tomar en cuenta (Molisch, 2022).

- **PSK (Keying de Fase):** En este esquema, la fase de la onda portadora se modifica de acuerdo con los datos transmitidos, donde una variante más eficiente, QPSK (Quadrature PSK), permite la transmisión de dos bits por cada cambio de fase, mejorando la eficiencia espectral; este tipo de modulación se usa ampliamente en redes Wi-Fi y comunicaciones satelitales debido a su capacidad de soportar tasas de datos elevadas. (Stallings, 2013).
- **QAM (Modulación de Amplitud en Cuadratura):** Esta técnica combina cambios en la amplitud y fase de la señal para transmitir una mayor cantidad de datos por unidad de tiempo, siendo ampliamente utilizada en redes Wi-Fi modernas (802.11ac/ax) y en sistemas de comunicación celular como LTE y 5G. El uso de QAM en redes inalámbricas ha permitido el aumento significativo en lo que respecta a la capacidad de transmisión, facilitando velocidades de datos mayores a 1 Gbps. (Johnson, 2020).

Imagen 7: Métodos de modulación.
Fuente: Elaboración propia.

2.4. Propagación de ondas: obstáculos e interferencias.

La propagación de ondas en redes inalámbricas es un fenómeno complejo influenciado por diversos factores ambientales y arquitectónicos, donde la señal inalámbrica se transmite a través del espectro electromagnético y puede verse afectada por la presencia de obstáculos físicos, interferencias de otras fuentes y condiciones

atmosféricas, por lo tanto comprender estos factores es crucial para diseñar redes inalámbricas eficientes y mitigar posibles problemas de conectividad (Hasegawa et al., 2013).

Principios de Propagación de Ondas

Las ondas electromagnéticas utilizadas en las redes inalámbricas pueden propagarse de diversas formas dependiendo del medio y los obstáculos que encuentran en su trayecto. A continuación, se describen los principales mecanismos de propagación:

- **Propagación en línea de vista (LOS, Line of Sight):** Se produce cuando no hay obstáculos entre el transmisor y el receptor, lo que permite una transmisión eficiente y sin pérdidas significativas de la señal. Es el tipo de propagación ideal en entornos abiertos o para enlaces de radiofrecuencia a larga distancia (Devoti y Filippini, 2020).
- **Propagación por difracción:** Ocurre cuando una onda electromagnética encuentra un obstáculo en su trayectoria y se dobla alrededor de este, por lo tanto, dicho fenómeno permite que la señal alcance áreas que no estarían accesibles en una propagación en línea de vista, aunque con una pérdida de potencia significativa.
- **Propagación por reflexión y dispersión:** Se da cuando las ondas de radio rebotan en superficies como edificios, el suelo o estructuras metálicas. Este fenómeno puede ser beneficioso para mantener la conectividad en entornos urbanos, donde las señales reflejadas pueden llegar a lugares donde no hay línea de vista directa (Jiang et al., 2019).
- **Propagación por absorción:** Se produce cuando la energía de la señal es absorbida parcial o totalmente por el material de los obstáculos, reduciendo la intensidad de la señal que llega al receptor, donde algunos materiales como el concreto, el metal y el agua, generan altos niveles de absorción, afectando la calidad de la conexión inalámbrica.
- **Propagación por multitrayectoria:** Se genera cuando la señal toma múltiples caminos hasta llegar al receptor debido a reflexiones, refracciones y difracciones en el entorno, este tipo de propagación puede causar interferencia constructiva o destructiva, afectando la calidad de la comunicación inalámbrica, ya que en algunos casos, las tecnologías modernas como MIMO (Multiple Input Multiple Output) permiten aprovechar la propagación por multitrayectoria para mejorar la eficiencia del canal (Beļinskis et al., 2023).

Algunos de estos principios también pueden afectar el desvanecimiento de las señales.

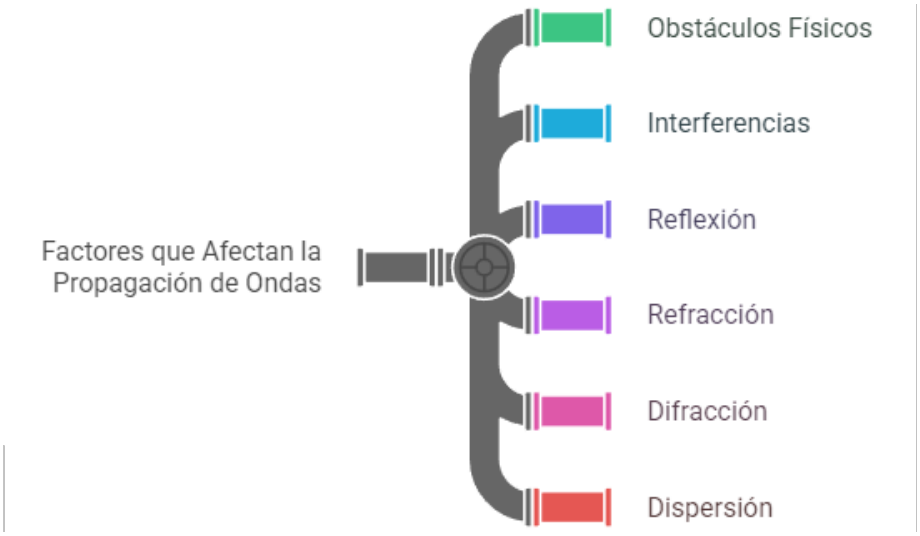

Imagen 8: Factores que afectan la propagación de ondas electromagnéticas.
Fuente: Elaboración propia.

Obstáculos físicos

Los obstáculos pueden debilitar o bloquear completamente la transmisión de la señal, donde la atenuación de esta depende del tipo, tamaño y composición del obstáculo, así como de la frecuencia de la onda electromagnética utilizada. Entre los principales tipos de obstáculos se encuentran:

- **Edificios y estructuras urbanas:** Las construcciones pueden generar sombra radioeléctrica y reducir la calidad de la conexión inalámbrica y además, los materiales de construcción juegan un papel clave en la propagación de las ondas de radio: el concreto y el metal pueden reflejar o absorber la señal, mientras que el vidrio puede permitir cierto nivel de penetración. Es necesario mencionar que, en los entornos urbanos densos, los edificios altos pueden provocar pérdidas de señal significativas debido a la dispersión y absorción (Hasegawa et al., 2013).
- **Vegetación:** Los árboles y hojas pueden absorber o reflejar las ondas de radio, afectando la calidad de la transmisión, especialmente en redes de baja frecuencia, donde la atenuación depende de la densidad de la vegetación, la humedad en las hojas y la frecuencia de la señal utilizada, donde algunos estudios han demostrado que las frecuencias más altas, como las utilizadas en redes 5G y mmWave, son particularmente vulnerables a la absorción de la vegetación.

- **Interferencia de otros dispositivos:** Las señales de redes Wi-Fi, Bluetooth, hornos de microondas y otros dispositivos electrónicos pueden generar interferencias que degradan el rendimiento de la red, por lo tanto, esto es especialmente problemático en el espectro de 2.4 GHz, donde operan múltiples tecnologías de comunicación inalámbrica y la congestión del espectro puede generar ruido y colisiones de señal, reduciendo la velocidad y estabilidad de la conexión (Niknam et al., 2018).
    - **Condiciones atmosféricas:** Factores como la lluvia, la niebla y la humedad pueden afectar la propagación de las ondas electromagnéticas, en particular, las redes que operan en bandas de frecuencia alta, como mmWave (30 GHz - 300 GHz), experimentan una mayor atenuación debido a la absorción de la señal por las partículas de agua en la atmósfera, de tal forma que esto puede limitar el alcance efectivo de las conexiones inalámbricas y afectar la estabilidad de la señal en climas adversos (Beļinskis et al., 2023).
    - **Objetos en movimiento:** Vehículos, personas y otros objetos en movimiento pueden causar fluctuaciones en la señal inalámbrica debido a la dispersión y la interferencia por multitrayectoria. En entornos altamente dinámicos, como aeropuertos y estaciones de tren, la calidad de la señal puede verse afectada por la constante variación en la disposición de los obstáculos y el efecto Doppler en las ondas de radio.

Mecanismos de Mitigación de Interferencias

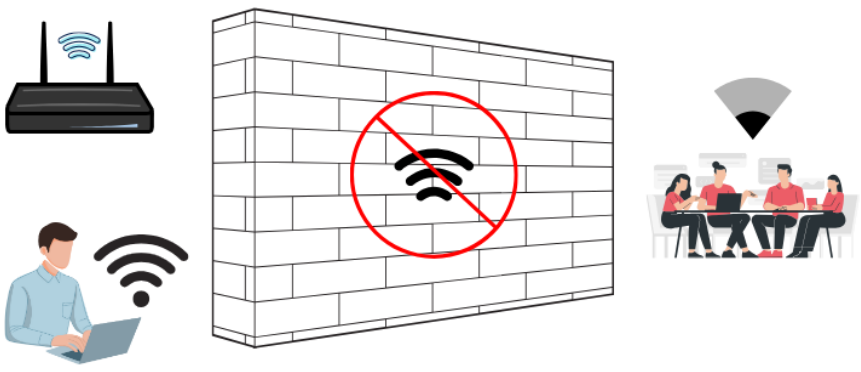

Imagen 9: Obstáculos e interferencias en conexiones inalámbricas.
Fuente: Elaboración propia.

Para reducir los efectos negativos de los obstáculos y la interferencia en redes inalámbricas, se pueden implementar diversas estrategias:

- **Selección dinámica de canales:** Permite cambiar automáticamente a un canal menos congestionado.
- **Uso de tecnologías MIMO (Multiple Input Multiple Output):** Mejora la recepción de señales al utilizar múltiples antenas.
- **Configuración de potencias de transmisión:** Ajustar la potencia de transmisión según el entorno ayuda a minimizar interferencias.
- **Redes de malla (Mesh Networks):** Facilitan rutas alternativas para los datos, evitando zonas con alto nivel de interferencia (Yang et al., 2019).

La comprensión de estos fenómenos es esencial para el diseño y despliegue de redes inalámbricas eficientes y de alto rendimiento en diversos entornos.

2.5. Componentes básicos.

Las redes inalámbricas han revolucionado la comunicación moderna al eliminar la necesidad de conexiones físicas y proporcionar una movilidad sin precedentes. Para comprender el funcionamiento de estas redes, es esencial conocer sus componentes básicos, los cuales permiten la transmisión y recepción de datos a través de medios inalámbricos, donde estos componentes incluyen puntos de acceso, dispositivos terminales, antenas, protocolos de comunicación y mecanismos de seguridad (Cecílio y Furtado, 2014).

Puntos de Acceso (Access Points)

El punto de acceso (AP) es un dispositivo esencial en las redes inalámbricas que permite la conexión de dispositivos finales a la red y opera como un puente entre la red cableada y la inalámbrica, gestionando la comunicación y asegurando la conectividad entre los nodos de la red; pueden operar en diferentes modos, como infraestructura o ad hoc, dependiendo de los requisitos de la red y su configuración (Carthern et al., 2015).

Dispositivos Terminales

Los dispositivos terminales incluyen computadoras, teléfonos inteligentes, tabletas y cualquier otro equipo que pueda conectarse a una red inalámbrica, por lo tanto, estos dispositivos contienen tarjetas de red inalámbrica (WLAN) que les permiten establecer una conexión con los puntos de acceso y comunicarse con otros nodos dentro de la red (Singh, 2019).

Antenas

Las antenas desempeñan un papel fundamental en la transmisión y recepción de señales inalámbricas, ya que existen distintos tipos de antenas utilizadas en redes inalámbricas, incluyendo:

- **Antenas omnidireccionales:** Emiten señales en todas direcciones y son utilizadas en redes Wi-Fi domésticas y comerciales.
- **Antenas direccionales:** Enfocan la señal en una dirección específica, proporcionando un mayor alcance y estabilidad de conexión (Dubrawsky, 2010).

2.6. Resumen Ejecutivo del Capítulo

Este capítulo abordó los fundamentos técnicos esenciales de la comunicación inalámbrica, explicando cómo las señales electromagnéticas permiten la transmisión de datos sin cables. Se describen las bandas de frecuencia más utilizadas (2.4 GHz, 5 GHz, 6 GHz y Sub-1 GHz), así como el espectro radioeléctrico y su regulación internacional. Se presentan los principales métodos de modulación (ASK, FSK, PSK, QAM) y técnicas de codificación (fuente y canal), fundamentales para garantizar la integridad de los datos transmitidos. El capítulo también analiza los fenómenos que afectan la propagación de ondas, como la reflexión, difracción, absorción y multitrayectoria, así como los obstáculos físicos que pueden interferir en la señal. Finalmente, se describen los componentes básicos de una red inalámbrica: puntos de acceso, dispositivos terminales y antenas, destacando su importancia en la eficiencia y alcance de la red. Un caso de estudio ilustra la planificación de una red inalámbrica en una empresa con múltiples pisos.

2.7. Caso de estudio.

Una empresa necesita implementar una red inalámbrica en un edificio de tres plantas, donde la red debe soportar múltiples dispositivos simultáneamente, minimizar interferencias y garantizar la seguridad de los datos. Actualmente, la empresa enfrenta problemas de conectividad en ciertas áreas, lo que afecta la productividad de los empleados, y se requiere una estrategia eficiente para la colocación de puntos de acceso, la selección de bandas de frecuencia y la aplicación de protocolos de seguridad adecuados.

El objetivo es analizar los factores clave en el diseño e implementación de una red inalámbrica en un entorno corporativo de múltiples niveles, considerando aspectos como cobertura, interferencias y seguridad.

Preguntas para el análisis:

1. ¿Qué factores deben considerarse al elegir la banda de frecuencia para la red inalámbrica y cómo afectan la cobertura y la interferencia?
2. ¿Cuáles son las ventajas y desventajas de utilizar un diseño de red con múltiples puntos de acceso en comparación con un único punto centralizado?
3. ¿Qué medidas de seguridad se deben implementar para proteger la red contra accesos no autorizados y ataques externos?

2.8. Resumen Ejecutivo del Capítulo

Este capítulo abordó los fundamentos técnicos esenciales de la comunicación inalámbrica, explicando cómo las señales electromagnéticas permiten la transmisión de datos sin cables. Se describen las bandas de frecuencia más utilizadas (2.4 GHz, 5 GHz, 6 GHz y Sub-1 GHz), así como el espectro radioeléctrico y su regulación internacional. Se presentan los principales métodos de modulación (ASK, FSK, PSK, QAM) y técnicas de codificación (fuente y canal), fundamentales para garantizar la integridad de los datos transmitidos. El capítulo también analizó los fenómenos que afectan la propagación de ondas, como la reflexión, difracción, absorción y multitrayectoria, así como los obstáculos físicos que pueden interferir en la señal. Finalmente, se describen los componentes básicos de una red inalámbrica: puntos de acceso, dispositivos terminales y antenas, destacando su importancia en la eficiencia y alcance de la red, donde en un caso de estudio se ilustra la planificación de una red inalámbrica en una empresa con múltiples pisos.

2.9. Evaluación del capítulo.

¿Qué rango de frecuencia es más utilizado por redes Wi-Fi tradicionales?

a) 1 GHz.
b) 2.4 GHz.
c) 10 GHz.
d) 6 GHz.

¿Cuál es un método común de modulación?

a) TDM.
b) FSK.
c) CDMA.
d) OFDM.

¿Cuál de los siguientes es un obstáculo común en la propagación de ondas inalámbricas?

a) Un césped.
b) Una pared de concreto.
c) Una ventana abierta.
d) Un dispositivo móvil.

¿Qué dispositivo actúa como intermediario entre dispositivos inalámbricos y redes cableadas?

a) Router.
b) Punto de acceso.
c) Antena.
d) Switch.

¿Qué fenómeno ocurre cuando una señal se dobla por un obstáculo?

a) Difracción
b) Reflexión
c) Absorción
d) Dispersión

REFERENCIAS BIBLIOGRÁFICAS

Beļinskis, R., Bogdanovs, N., Titovičs, J., Ipatovs, A., Klūga, J., & Ćulkovs, D. (2023). Propagation Losses Algorithm for Indoor Wireless Sensor Network. Progress in Electromagnetic Research Symposium (PIERS), 1772-1778. https://doi.org/10.1109/PIERS59004.2023.10221251

Carthern, C., Wilson, W., Bedwell, R., & Rivera, N. (2015). Cisco Networks: Engineers' Handbook of Routing, Switching, and Security with IOS, NX-OS, and ASA (Primera ed.). Apress. https://doi.org/10.1007/978-1-4842-0859-5

Cecílio, J., & Furtado, P. (2014). Wireless Sensor Networks: Concepts and Components. Springer, Cham, 5-25. https://doi.org/10.1007/978-3-319-09280-5

Devoti, F., & Filippini, I. (2020). Planning mm-Wave Access Networks Under Obstacle Blockages: A Reliability-Aware Approach. IEEE/ACM Transactions on Networking, 28(5), 2203-2214. https://doi.org/10.1109/TNET.2020.3006926

Dubrawsky, I. (2010). Eleventh Hour Network+: Exam N10-004 Study Guide. Syngress. https://doi.org/10.1016/C2009-0-20666-0

Hasegawa, G., Ise, Y., Taniguchi, Y., & Nakano, H. (2013). Effect of Radio Wave Obstruction by Obstacles on Performance of IEEE 802.16j Wireless Multi-Hop Relay Networks. International Journal on Advances in Networks and Services, 6(1 & 2), 17-26. https://www.iariajournals.org/networks_and_services/tocv6n12.html

Jiang, X., Shokri-Ghadikolaei, H., Fischione, C., & Pang, Z. (2019). A Simplified Interference Model for Outdoor Millimeter-wave Networks. Mobile Networks and Applications, 24, 983-990. https://doi.org/10.1007/s11036-018-1030-2

Johnson, A. (2020). Wireless Concepts. Cisco Press: https://www.ciscopress.com/articles/printerfriendly/2999384

Molisch, A. (2022). Wireless Communications: From Fundamentals to Beyond 5G (3rd ed.). Wiley-IEEE Press. https://doi.org/978-1-119-11721-6

Niknam, S., Barazideh, R., & Natarajan, B. (2018). Cross-Layer Interference Modeling for 5G mmWave Networks in the Presence of Blockage. IEEE/2018 IEEE 88th Vehicular Technology

Conference (VTC-Fall), 1-5. https://doi.org/10.1109/VTCFall.2018.8690830

Proakis, J., & Salehi, M. (2007). Digital Communications (Quinta ed.). McGraw-Hill Education. https://doi.org/978-0072957167

Rappaport, T., Heath, R., Robert, D., & James, M. (2014). Millimeter Wave Wireless Communications. Prentice Hall. https://doi.org/978-0-13-217228-8

Rappaport, T., Xing, Y., Kanhere, O., Ju, S., Madanayake, A., Mandal, S., . . . Trichopoulos, G. (2019). Wireless Communications and Applications Above 100 GHz: Opportunities and Challenges for 6G and Beyond. IEEE Access, 7, 78729-78757. https://doi.org/https://doi.org/10.1109/ACCESS.2019.2921522

Singh, M. (2019). Node-to-Node Approaching in Wireless Mesh Connectivity (Primera ed.). Springer Singapore. https://doi.org/10.1007/978-981-13-0674-7

Stallings, W. (2013). Data and Computer Communications (Décima ed.). Pearson. https://doi.org/978-0133506488

Yang, H., Xiao, Z., Hou, H., Fan, F., Li, P., Wen, W., . . . Liu, L. (2019). Research on Power Wireless Private Network Planning Technology Considering Propagation Model Correction Part Two Applications and Explorations. Procedia Computer Science, 155, 763-767. https://doi.org/10.1016/j.procs.2019.08.111

Capítulo3: Estándares y Protocolos

Los estándares y protocolos son fundamentales para garantizar la interoperabilidad, seguridad y eficiencia en las redes inalámbricas, desde la adopción masiva de Wi-Fi hasta el auge de las redes móviles LTE y 5G, donde las tecnologías inalámbricas han transformado la forma de como nos conectamos y comunicamos. Esta evolución ha sido impulsada por el desarrollo de diversos estándares y protocolos que garantizan la interoperabilidad, eficiencia y seguridad en las comunicaciones inalámbricas (Kurose y Ross, 2021). Este capítulo explora en detalle los estándares IEEE 802.11, que soportan diferentes generaciones de Wi-Fi, así como las tecnologías de corto alcance como Bluetooth y Zigbee, diseñadas para aplicaciones como la domótica e IoT, además, se analiza la evolución de las redes móviles LTE hacia 5G, destacando su impacto en la conectividad global, los roles de organismos reguladores y certificaciones en el aseguramiento de la calidad y el cumplimiento normativo. Este conocimiento permitirá a los lectores comprender los aspectos técnicos y regulatorios clave para diseñar y gestionar redes inalámbricas efectivas y seguras.

Objetivos del capítulo:

- Identificar y analizar las características principales de los estándares de redes inalámbricas IEEE 802.11 (Wi-Fi), Bluetooth y Zigbee.
- Comprender las tecnologías LTE y 5G en el contexto de las redes móviles.
- Realizar una comparativa entre los estándares inalámbricos mencionados, evaluando sus ventajas, limitaciones y aplicaciones.
- Reconocer la importancia de las certificaciones y organismos reguladores en la implementación y uso de tecnologías inalámbricas.

3.1. IEEE 802.11: Wi-Fi

Los estándares IEEE 802.11, comúnmente conocidos como Wi-Fi, han evolucionado significativamente a lo largo de los años, y cada iteración introduce mejoras para satisfacer las crecientes demandas de conectividad inalámbrica, estos estándares, incluidos los 802.11a/b/g/n/ac/ax, se han desarrollado para mejorar las velocidades de datos, la cobertura y la confiabilidad, y se adaptan a diversas aplicaciones, desde el uso personal hasta el industrial.

El estándar más reciente, el 802.11ax, también conocido como Wi-Fi 6, ofrece mejoras sustanciales en cuanto a latencia y confiabilidad, lo que lo hace adecuado para aplicaciones más exigentes Experimental. A continuación, se presenta un análisis detallado de estos estándares.

IEEE 802.11a/b/g

Los estándares IEEE 802.11a y 802.11b fueron los primeros en establecerse en el mercado, mientras que el 802.11b operaba en la banda de 2.4 GHz con velocidades máximas de 11 Mbps, 802.11a utilizaba la banda de 5 GHz, alcanzando hasta 54 Mbps, posteriormente, 802.11g combinó la compatibilidad de 802.11b con la velocidad de 802.11a, donde dichos estándares iniciales sirvieron como base para el desarrollo de tecnologías más avanzadas (Johnson, 2020).

IEEE 802.11n

Introducido en 2009, este estándar mejoró significativamente las velocidades y la cobertura gracias a la tecnología MIMO (Multiple Input, Multiple Output), que permite transmitir y recibir datos por múltiples antenas, aumentando la eficiencia del espectro, y además incorporó el uso de canales de 40 MHz, duplicando el ancho de banda disponible y alcanzando velocidades de hasta 600 Mbps, por lo tanto se puede mencionar que su capacidad de operar en bandas de 2.4 GHz y 5 GHz proporcionó flexibilidad en diversos entornos (IEEE, 2025).

IEEE 802.11ac

IEEE 802.11ac, conocido como Wi-Fi 5, este estándar mejoró el 802.11n al ofrecer velocidades de datos más altas gracias a anchos de banda de canales más amplios y a más transmisiones MIMO (Gajbhiye et al., 2024). Además, se puede mencionar que dicho estándar al enfocarse exclusivamente en la banda de 5 GHz marcó un hito, optimizando el rendimiento con el uso de canales de hasta 160 MHz y modulación de alta densidad (256-QAM), permitiendo velocidades de hasta 6.9 Gbps, haciéndolo ideal para aplicaciones de alta demanda como streaming 4K y videoconferencias (Wi-Fi Alliance, 2022).

IEEE 802.11ax

IEEE 802.11ax o Wi-Fi 6 introdujo mejoras significativas para entornos densos, como estadios o edificios empresariales, al incorporar OFDMA (Orthogonal Frequency-Division Multiple Access), que divide el canal en subcanales más pequeños para optimizar la transmisión, además incluyó MU-MIMO (Multi-User MIMO), permitiendo conexiones simultáneas múltiples con un mayor número de dispositivos, permitiendo al estándar alcanzar velocidades teóricas de 9.6 Gbps y mejorar la eficiencia energética de los dispositivos conectados (Wi-Fi Alliance, 2022).

IEEE 802.11be

Wi-Fi 7, también conocido como IEEE 802.11be, representa un salto significativo en la tecnología de redes inalámbricas, con el objetivo de satisfacer la creciente demanda de velocidades de datos más altas y una latencia más baja, con velocidades potenciales de hasta 30 Gbps, permitiendo introducir innovaciones como los anchos de canal de 320 MHz, el 4096-QAM y el funcionamiento multienlace (MLO), que mejoran la estabilidad y la eficiencia de la red. Esta tecnología está preparada para soportar diversas aplicaciones, incluidas las ciudades inteligentes, la telemedicina y la automatización industrial, al proporcionar conexiones inalámbricas rápidas y confiables (Murad et al., 2024).

Imagen 10: Línea de tiempo del estándar 802.11.
Fuente: Elaboración propia.

3.2. Bluetooth

Bluetooth, desarrollado por el SIG (Bluetooth Special Interest Group), es una tecnología diseñada para conexiones de corto alcance con bajo consumo de energía, permitiendo aplicaciones que van desde auriculares inalámbricos hasta sensores IoT.

Bluetooth 5.0, una de las versiones más recientes, ofrece velocidades de transferencia de hasta 2 Mbps y un alcance máximo de 240 metros en condiciones ideales, donde se puede desglosar una característica clave de Bluetooth, que es su capacidad para realizar conexiones punto a punto o redes en estrella, lo que lo hace ideal para dispositivos portátiles y accesorios de consumo (Bluetooth SIG, 2025).

Bluetooth LE (Low Energy), una variante de esta tecnología está diseñada específicamente para aplicaciones que requieren un consumo energético extremadamente bajo, como dispositivos médicos y wearables, además, Bluetooth Mesh extiende su funcionalidad al permitir comunicaciones en redes distribuidas, facilitando aplicaciones en iluminación inteligente y sistemas de seguridad.

3.3. Zigbee

Zigbee es una tecnología inalámbrica basada en el estándar IEEE 802.15.4, diseñada para aplicaciones que requieren bajo consumo de energía y comunicaciones de baja velocidad, la misma que opera principalmente en la banda de 2.4 GHz, aunque también admite otras frecuencias según la región. Su capacidad para crear redes mesh es una de sus principales fortalezas, ya que permite que los dispositivos actúen como repetidores, extendiendo la cobertura y mejorando la resiliencia de la red (Connectivity Standards Alliance, 2023).

Zigbee es ampliamente utilizado en aplicaciones de IoT, como la automatización del hogar, control de iluminación y sensores ambientales y su bajo consumo de energía permite que los dispositivos funcionen durante años con baterías estándar, aunque su velocidad de transmisión es relativamente baja (250 kbps), esto es suficiente para la mayoría de las aplicaciones de monitoreo y control.

Un aspecto importante de Zigbee es su interoperabilidad, garantizada por la Zigbee Alliance, que establece perfiles de aplicación estandarizados para diferentes casos de uso, donde facilita la integración de dispositivos de múltiples fabricantes en una misma red.

3.4. LTE y 5G para redes móviles

LTE (Long-Term Evolution)

LTE, representa un gran avance en las redes móviles de cuarta generación (4G). Su arquitectura está basada en IP, eliminando la dependencia de circuitos tradicionales para transmitir voz y datos, esto mejora la eficiencia espectral y reduce los costos operativos y permite velocidades de descarga teóricas de hasta 300 Mbps y 75 Mbps de subida, con latencias que rondan los 20-30 ms, lo que mejora significativamente la experiencia del usuario en aplicaciones en tiempo real como videoconferencias y juegos en línea (3GGP, 2023).

La tecnología LTE introduce características clave como:

- **Carrier Aggregation (CA):** Combina múltiples bandas de frecuencia para aumentar la capacidad y las velocidades.
- **MIMO:** Mejora la capacidad y cobertura mediante el uso de múltiples antenas.
- **VoLTE (Voice over LTE):** Permite realizar llamadas de voz a través de la red LTE con alta calidad.

LTE ha sido adoptado masivamente debido a su capacidad para satisfacer la creciente demanda de datos móviles, especialmente con el aumento del streaming y las aplicaciones intensivas en datos.

5G (Quinta Generación)

5G, es un estándar que redefine las capacidades de las redes móviles, diseñada para manejar la explosión de dispositivos conectados en el Internet de las Cosas (IoT), 5G ofrece una combinación sin precedentes de velocidad, latencia y capacidad, donde sus características principales incluyen:

- **Velocidades ultrarrápidas:** Hasta 10 Gbps en condiciones óptimas, habilitando aplicaciones como realidad virtual, realidad aumentada y streaming en 8K (Committed to connecting the world, 2020).
- **Latencia extremadamente baja:** Menor a 1 ms en configuraciones ideales, lo que es crucial para aplicaciones críticas como conducción autónoma y cirugía remota.
- **Densidad de dispositivos:** Soporte para hasta un millón de dispositivos conectados por kilómetro cuadrado, ideal para ciudades inteligentes y entornos IoT masivos.
- **Eficiencia energética:** Mejora la duración de la batería en dispositivos IoT, al tiempo que reduce el consumo energético de las estaciones base.

El despliegue de 5G se basa en tres bandas principales:

- **Banda baja:** Proporciona cobertura amplia con velocidades moderadas.
- **Banda media:** Equilibrio entre cobertura y capacidad.
- **Banda alta (mmWave):** Ofrece las mayores velocidades y capacidades, aunque con menor alcance y penetración.

5G no solo es una evolución tecnológica, sino una plataforma que impulsa la transformación digital en sectores como la salud, manufactura y transporte, abriendo posibilidades como el monitoreo remoto de pacientes, fábricas inteligentes y vehículos autónomos.

Comparativa entre tecnologías inalámbricas

Tabla 2 part.1: Comparativa entre tecnologías de redes inalámbrica

Características	**Wi-Fi**	**Bluetooth**	**Zigbee**
Rango (Aproximado)	10-100 m	Hasta 240 m	Hasta 100 m
Velocidad	Hasta 9.6 Gbps	2 Mbps	250 Kbps
Consumo energético	Medio	Bajo	Muy bajo
Frecuencia	2.4 GHz, 5 GHz	2.4 GHz	2.4 GHz
Aplicaciones	Hogar, oficina	Audio, dispositivos	IoT, domótica
Costo de implementación	Moderado	Bajo	Bajo

Fuente: Elaboración propia.

Tabla 3 part.2: Comparativa entre tecnologías de redes inalámbrica

Características	**LTE**	**5G**
Rango (Aproximado)	Amplio (Km)	Amplio (Km)
Velocidad	Hasta 300 Mbps	Hasta 10 Gbps
Consumo energético	Alto	Alto
Frecuencia	Varias bandas	Varias bandas
Aplicaciones	Redes móviles 4G	IoT, automatización, redes móviles
Costo de implementación	Alto	Alto

Fuente: Elaboración propia.

Wi-Fi destaca por su alta velocidad en aplicaciones locales, mientras que Bluetooth y Zigbee son ideales para redes de corto alcance con menor consumo energético, por otro lado LTE y 5G, ofrecen cobertura global y un rendimiento óptimo para comunicaciones móviles e IoT de alta densidad, aunque con mayores costos asociados.

3.5. Certificaciones y organismos reguladores

Para garantizar la interoperabilidad y el cumplimiento de normativas en los dispositivos inalámbricos, existen diversos organismos de certificación y regulación:

Wi-Fi Alliance

Es una organización global que certifica dispositivos para asegurar la interoperabilidad entre diferentes marcas y fabricantes, donde se garantiza que los productos cumplan con los estándares IEEE 802.11 y sean compatibles entre sí, permitiendo, además, la implementación de tecnologías, como Wi-Fi Direct y Wi-Fi 6E, para mejorar la experiencia del usuario (Wi-Fi Alliance, 2022).

Bluetooth SIG (Grupo de Interés Especial)

Bluetooth SIG es responsable del desarrollo, mantenimiento y promoción de los estándares Bluetooth, ofreciendo certificaciones para garantizar que los dispositivos Bluetooth sean seguros, interoperables y cumplan con las especificaciones técnicas, siendo esta, obligatoria para los fabricantes que desean utilizar el logotipo de Bluetooth en sus productos (Bluetooth SIG, 2025).

Zigbee Alliance

Ahora conocida como Connectivity Standards Alliance (CSA), esta organización establece estándares abiertos para dispositivos IoT y garantiza que los dispositivos sean interoperables y puedan integrarse fácilmente en redes existentes, por ejemplo, los perfiles de aplicación, como Zigbee Home Automation, son clave para la adopción masiva de esta tecnología (Connectivity Standards Alliance, 2023).

ITU (Unión Internacional de Telecomunicaciones)

La ITU regula el espectro radioeléctrico a nivel global, asignando frecuencias y estableciendo estándares internacionales para la comunicación inalámbrica, ya que permite evitar interferencias y garantizar el uso eficiente del espectro.

FCC (Comisión Federal de Comunicaciones)

La FCC regula el uso del espectro radioeléctrico en los Estados Unidos, donde los dispositivos inalámbricos deben cumplir con las normativas de la FCC para ser comercializados en el país, esto asegura que los equipos no interfieran con otras comunicaciones y operen dentro de los límites establecidos (Federal Communications Commission, 2025).

3GPP (Proyecto de Asociación para la 3ra Generación)

Desarrolla y mantiene los estándares para redes de telecomunicaciones móviles, incluyendo 2G (GSM), 3G (UMTS), 4G (LTE) y 5G (NR - New Radio), siendo una de las principales organizaciones responsables de la evolución de las tecnologías móviles a nivel global.

Las certificaciones generan ciertos beneficios, por ejemplo:

- **Interoperabilidad:** Garantizan que los dispositivos puedan comunicarse de manera efectiva, independientemente del fabricante.
- **Seguridad:** Aseguran que los equipos cumplen con las normativas de protección contra ciberataques y fallos.

- **Conformidad:** Facilitan el cumplimiento de regulaciones nacionales e internacionales, evitando sanciones.
- **Confianza del consumidor:** Incrementan la credibilidad de los productos en el mercado, fomentando su adopción.

Imagen 11: Organismos de certificación y regulación.
Fuente: Elaboración propia.

3.6. Caso de estudio

Una universidad planea renovar su red inalámbrica. Requiere alta velocidad en aulas, Bluetooth para geolocalización, y Zigbee para sensores IoT. Consideran usar Wi-Fi 6 y 5G para exteriores.

Tareas:

- Seleccionar estándares apropiados para Wi-Fi, Bluetooth y Zigbee.
- Comparar LTE vs 5G en cobertura y velocidad.
- Evaluar impacto de cada tecnología en consumo energético.
- Consultar regulaciones locales para uso de espectro.

Preguntas para el análisis:

1. ¿Qué ventajas tiene Wi-Fi 6 frente a Wi-Fi 5?
2. ¿Por qué Zigbee es ideal para sensores IoT?
3. ¿Qué limitaciones presenta el uso de 5G?
4. ¿Qué organismos certifican dispositivos inalámbricos?

3.7. Resumen Ejecutivo del Capítulo

Este capítulo examinó los estándares y protocolos que garantizan la interoperabilidad, eficiencia y seguridad en las redes inalámbricas, donde se analizaron las versiones del estándar IEEE 802.11 (Wi-Fi), desde 802.11a/b/g hasta Wi-Fi 7 (802.11be), detallando sus mejoras en velocidad, cobertura y eficiencia. También se presentaron tecnologías de corto alcance como Bluetooth, incluyendo su versión Low Energy y Bluetooth Mesh, y Zigbee, utilizado ampliamente en IoT por su bajo consumo y capacidad de red mallada. En redes móviles, se explican LTE y 5G, destacando sus aplicaciones, ventajas en velocidad y baja latencia, por último, el capítulo compara las características de estas tecnologías, su rango, velocidad, frecuencia y consumo energético, y, además, se describen los organismos certificadores como Wi-Fi Alliance, Bluetooth SIG, Zigbee Alliance, ITU, FCC y 3GPP, que aseguran la conformidad técnica y regulatoria. Un caso de estudio ilustra la selección tecnológica para renovar una red universitaria multiservicio.

3.8. Evaluación del capítulo

¿Cuál es la velocidad máxima teórica de Wi-Fi 6?

a) 6.9 Gbps
b) 9.6 Gbps
c) 2 Mbps
d) 10 Gbps

¿Qué tecnología utiliza Zigbee para formar redes?

a) OFDMA
b) MIMO
c) Redes mesh
d) MU-MIMO

¿Cuál es la principal ventaja de 5G frente a LTE?

a) Mayor cobertura
b) Velocidades más altas
c) Menor costo de implementación
d) Consumo energético reducido

¿Qué organización regula el espectro radioeléctrico a nivel global?

a) Wi-Fi Alliance
b) ITU
c) FCC
d) Bluetooth SIG

¿Qué característica distingue a Zigbee?

a) Alta velocidad

b) Bajo consumo
c) Uso de 5GHz
d) Alto costo

REFERENCIAS BIBLIOGRÁFICAS

3GGP. (2023). Release 18. 3rd Generation Partnership Project: https://www.3gpp.org/specifications-technologies/releases/release-18

Bluetooth SIG. (2025). Bluetooth Technology Overview. Bluetooth: https://www.bluetooth.com/learn-about-bluetooth/tech-overview/

Committed to connecting the world. (2020). IMT-2020 (a.k.a. "5G"). ITU: https://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2020/Pages/default.aspx

Connectivity Standards Alliance. (2023). CSA Conectivity Standards Alliance. Zigbee Specification: https://csa-iot.org/wp-content/uploads/2023/04/05-3474-23-csg-zigbee-specification-compressed.pdf

Federal Communications Commission. (2025). Federal Communications Commission. Radio Spectrum Allocation: https://www.fcc.gov/engineering-technology/policy-and-rules-division/general/radio-spectrum-allocation

Gajbhiye, P., Singh, S., & Sharma, M. (2024). Computationally optimized multi-port antenna systems for WLAN/Wi-Fi (IEEE 802.11a/h/j/n/ac/ax), 5G (mid-band), and UWB applications. International Journal Of Communication Systems, 38. https://doi.org/doi.org/10.1002/dac.5985

IEEE. (2025). The Evolution of Wi-Fi Technology and Standards. IEEE STANDARDS ASSOCIATON: https://standards.ieee.org/beyond-standards/the-evolution-of-wi-fi-technology-and-standards/

Johnson, A. (2020). Wireless Concepts. Cisco Press: https://www.ciscopress.com/articles/printerfriendly/2999384

Kurose, J., & Ross, K. (2021). Computer Networking: A Top-Down Approach (8 th. ed.). Pearson Education Limited. https://doi.org/978-1-292-40546-9

Murad, S., Badeel, R., Abdal, B., Rahman, T., & Al-Quraishi, T. (2024). Introduction to Wi-Fi 7: A Review of History, Applications, Challenges, Economical Impact and Research Development. Mesopotamian Journal of Computer Science, 2024, 110-121. https://doi.org/10.58496/MJCSC/2024/009

Wi-Fi Alliance. (2022). Wi-Fi Alliance 2022 Wi-Fi trends. Wi-Fi Alliance: https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-2022-wi-fi-trends

Capítulo4: Consideraciones para el Diseño e Implementación de Redes Inalámbricas

El diseño y la implementación de redes inalámbricas constituyen procesos esenciales para garantizar una conectividad eficiente, estable

y segura en los entornos tecnológicos actuales, por lo tanto, en esta sección se abordan las consideraciones fundamentales que deben contemplarse al planificar y configurar una red inalámbrica, tales como la cobertura, la capacidad operativa y los aspectos de seguridad. Asimismo, se examina el uso de herramientas especializadas para el análisis y la planificación de redes, junto con los pasos técnicos necesarios para la correcta configuración de dispositivos como puntos de acceso y routers. La adecuada instalación y la ejecución de pruebas de funcionamiento resultan determinantes para asegurar el rendimiento óptimo de la red, mientras que la identificación y resolución de problemas comunes son clave para mantener su operatividad a largo plazo. Este capítulo ofrece un enfoque práctico y detallado, basado en las mejores prácticas del sector y respaldado por literatura actualizada, con el objetivo de proporcionar a los profesionales las herramientas necesarias para implementar redes inalámbricas de manera exitosa y sostenible. (Kurose y Ross, 2021).

Objetivos:

- Comprender las consideraciones esenciales para diseñar redes inalámbricas, incluyendo cobertura, capacidad y seguridad.
- Identificar y utilizar herramientas de análisis y planificación para optimizar redes inalámbricas.
- Aprender a configurar puntos de acceso y routers inalámbricos de manera efectiva.
- Desarrollar habilidades para la instalación y pruebas de funcionamiento de redes inalámbricas.
- Resolver problemas comunes en redes inalámbricas mediante técnicas probadas.

4.1. Aspectos relevantes para el diseño de redes inalámbricas: cobertura, capacidad y seguridad

Cobertura

La cobertura de una red inalámbrica está determinada por la potencia de transmisión, la sensibilidad de recepción de los dispositivos y las características físicas del entorno, factores como paredes, muebles, equipos electrónicos y la cantidad de usuarios afectan significativamente la calidad de la señal (Ekahau, 2025).

Para garantizar una cobertura óptima, es esencial lo siguiente:

1. Realizar un estudio de sitio para identificar las áreas con baja señal, las zonas de interferencia y los puntos de alta densidad de usuarios.
2. Usar antenas direccionales u omnidireccionales según las necesidades específicas del área.
3. Minimizar la interferencia de otras redes utilizando canales no superpuestos y configurando adecuadamente la potencia de salida de los dispositivos.

Tecnologías como Wi-Fi 6 (802.11ax) ofrecen capacidades avanzadas para manejar entornos densos, aumentando la eficiencia del espectro disponible.

Capacidad

Según Bellalta (2016), menciona que, la capacidad de una red se refiere al número de dispositivos que pueden conectarse y operar simultáneamente sin experimentar una disminución significativa en el rendimiento, por lo tanto, existen varios factores que juegan un papel importante con la capacidad, tales como:

1. **Ancho de banda disponible:** La capacidad total de la red se divide entre todos los usuarios conectados, estándares modernos como Wi-Fi 6 permiten un uso más eficiente del espectro, habilitando transmisiones simultáneas a varios usuarios mediante tecnologías como OFDMA (Orthogonal Frequency Division Multiple Access).
2. **Planificación del tráfico:** Es esencial priorizar aplicaciones críticas mediante QoS (Quality of Service) para evitar la congestión de la red.
3. **Escalabilidad:** Diseñar la red con la flexibilidad necesaria para admitir un mayor número de dispositivos en el futuro.

Adicionalmente, las redes de malla ("mesh networks") pueden distribuir la carga entre múltiples puntos de acceso, mejorando la capacidad general.

Seguridad

Según Oppenheimer (2004), menciona que la seguridad es una de las consideraciones más críticas en el diseño de redes inalámbricas, donde las amenazas comunes incluyen ataques de intermediarios (man-in-the-middle), redes falsas ("rogue APs") y la interceptación de datos, y para mitigar estos riesgos, se recomienda:

1. **Uso de protocolos de cifrado:** WPA3 es el estándar más avanzado, proporcionando mayor protección frente a ataques de fuerza bruta y garantizando la confidencialidad de los datos.
2. **Implementación de VLANs:** Separar el tráfico de diferentes tipos de usuarios o dispositivos (por ejemplo, invitados y personal) para limitar el alcance de posibles ataques.
3. **Control de acceso:** Utilizar autenticación basada en 802.1X con un servidor RADIUS para verificar la identidad de los dispositivos y usuarios antes de permitirles el acceso.
4. **Auditorías periódicas:** Revisar regularmente la configuración de seguridad y los registros de actividad para detectar y responder rápidamente a incidentes.

Con el avance de las amenazas cibernéticas, también es importante educar a los usuarios sobre buenas prácticas de seguridad, como no compartir contraseñas y evitar conectarse a redes desconocidas.

4.2. Herramientas de análisis y planificación

Las herramientas de análisis y planificación desempeñan un papel crucial en el diseño e implementación de redes inalámbricas, las mismas que permiten evaluar la cobertura, capacidad y rendimiento de la red, así como identificar problemas potenciales antes de que ocurran, por lo tanto, se detallan algunas de las herramientas más destacadas:

Tabla 4 part.1: Comparación de Herramientas para Análisis y Optimización de Redes Wi-Fi

Característica	**Ekahau Site Survey**	**NetSpot**	**SolarWinds Wi-Fi Analyzer**	**AirMagnet Survey**
Propósito Principal	Diseño y optimización de redes Wi-Fi empresariales	Análisis de cobertura Wi-Fi y optimización	Monitoreo y análisis de redes Wi-Fi	Análisis y auditoría de redes Wi-Fi
Tipo de Usuario	Profesionales y empresas	Usuarios SOHO	Administradores de red y empresas	Profesionales y empresas
Compatibilidad	Windows, macOS	Windows, macOS	Windows	Windows
Generación de Mapas de Cobertura	Sí, con mapas de calor avanzados	Sí, con mapas de calor	No incluye mapas de cobertura avanzados	Sí, mapas detallados de cobertura
Soporte para Redes 2.4GHz / 5GHz	Sí	Sí	Sí	Sí
Soporte para Wi-Fi 6	Sí	Sí	Sí	Sí
Adaptador Especializado	Sí	No	No	Sí
Capacidad de Planificación de Redes	Sí	No	No	Sí

Análisis de Interferencias	Sí	No	Sí	Sí
Análisis de Canales	Sí	Sí	Sí	Sí
Monitoreo en Tiempo Real	Sí	No	Sí	Sí
Soporte para Seguridad Wi-Fi	Sí	Sí	Sí	Sí
Costo	Alto	Bajo	Medio	Alto

Fuente: Elaboración propia.

Tabla 5 part.2: Comparación de Herramientas para Análisis y Optimización de Redes Wi-Fi

Característica	**HeatMapper**	**TamoGraph Site Survey**	**Wireshark**
Propósito Principal	Mapeo de cobertura Wi-Fi	Planificación y optimización de redes Wi-Fi	Captura y análisis de tráfico de red
Tipo de Usuario	Usuarios domésticos	Profesionales y empresas	Ingenieros de red y seguridad
Compatibilidad	Windows	Windows, macOS	Windows, macOS, Linux
Generación de Mapas de Cobertura	Sí, pero limitado	Sí, mapas de calor avanzados	No
Soporte para Redes 2.4GHz / 5GHz	Sí	Sí	Sí
Soporte para Wi-Fi 6	No	Sí	No

Adaptador Especializado	No	Sí	No
Capacidad de Planificación de Redes	No	Sí	No
Análisis de Interferencias	No	Sí	Sí (Análisis de tráfico)
Análisis de Canales	No	Sí	No
Monitoreo en Tiempo Real	No	Sí	Sí
Soporte para Seguridad Wi-Fi	No	Sí	Sí
Costo	Gratuito	Medio-Alto	Gratuito

Fuente: Elaboración propia.

Tabla 6 part.3: Comparación de Herramientas para Análisis y Optimización de Redes Wi-Fi

Característica	**inSSIDer**	**WiFi Analyzer**	**Homedale**
Propósito Principal	Análisis de canales Wi-Fi e interferencias	Escaneo básico de redes Wi-Fi	Monitoreo y análisis de redes Wi-Fi
Tipo de Usuario	Pequeñas empresas y avanzados	Usuarios domésticos	Usuarios domésticos y avanzados
Compatibilidad	Windows, macOS	Windows	Windows, macOS
Generación de Mapas de Cobertura	No	No	No
Soporte para Redes 2.4GHz / 5GHz	Sí	Sí	Sí

Soporte para Wi-Fi 6	Sí	No	No
Adaptador Especializado	No	No	No
Capacidad de Planificación de Redes	No	No	No
Análisis de Interferencias	Sí	No	No
Análisis de Canales	Sí	Sí	Sí
Monitoreo en Tiempo Real	Sí	Sí	Sí
Soporte para Seguridad Wi-Fi	Sí	No	No
Costo	Medio	Gratuito	Gratuito

Fuente: Elaboración propia.

4.3. Beneficios del uso de herramientas de análisis y planificación.

Optimización de recursos

Estas herramientas permiten identificar la ubicación óptima de los puntos de acceso y routers, asegurando una distribución eficiente de los recursos para maximizar el rendimiento y reducir costos innecesarios.

Reducción de interferencias

Al analizar el espectro de frecuencias, las herramientas identifican fuentes de interferencia y recomiendan configuraciones óptimas de canales y potencias de transmisión, mejorando la estabilidad de la red.

Planificación a futuro

Ayudan a prever el crecimiento de la red, permitiendo una planificación escalable y adaptable a nuevas demandas tecnológicas o aumentos en la densidad de usuarios.

Detección y resolución proactiva de problemas

Estas herramientas identifican áreas problemáticas, como zonas con baja intensidad de señal o dispositivos que generan cuellos de botella, permitiendo resolverlos antes de que afecten la experiencia del usuario.

Generación de informes detallados

Proveen datos y análisis que facilitan la toma de decisiones informadas sobre actualizaciones o rediseños de la red.

Ahorro de tiempo

Automatizan procesos complejos como el análisis de cobertura y el diagnóstico de problemas, reduciendo significativamente el tiempo requerido para implementar y mantener la red.

Mejora en la experiencia del usuario

Una red bien diseñada y optimizada garantiza velocidades consistentes, menor latencia y conexiones estables, lo que mejora la satisfacción de los usuarios finales.

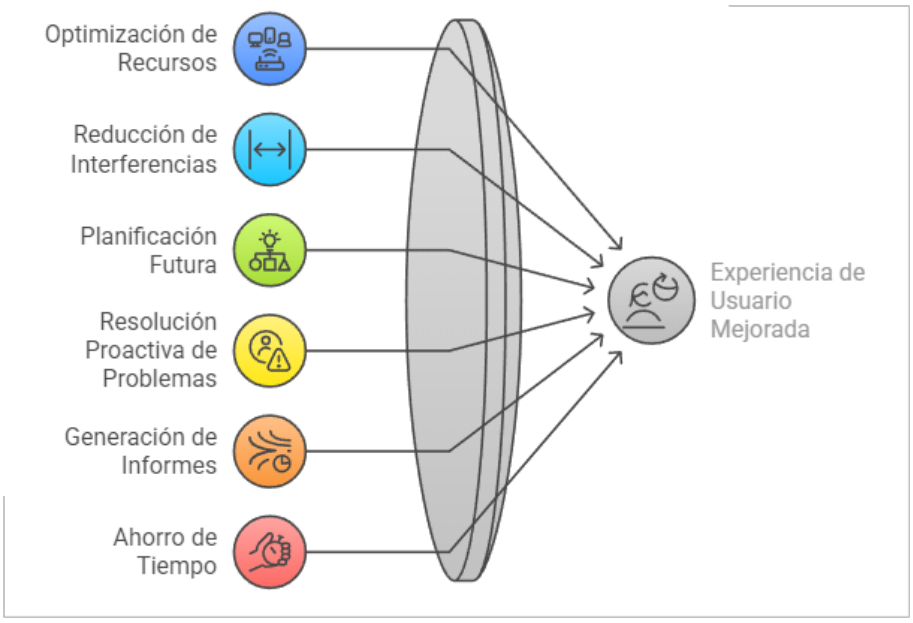

Imagen 12: Beneficios en el uso de herramientas para las redes de datos
Fuente: Elaboración propia.

Con base a lo mencionado se puede establecer que estas herramientas son fundamentales para garantizar que las redes inalámbricas cumplan con los estándares de rendimiento, seguridad y escalabilidad requeridos en entornos modernos.

4.4. Sugerencias para la configuración de puntos de acceso y routers inalámbricos

Puntos de acceso (AP)

Configurar un punto de acceso es un paso esencial para garantizar el rendimiento óptimo de la red, de los cuales, se establecen los pasos más importantes:

1. **Selección del canal:** Elegir el canal adecuado minimiza las interferencias. Por ejemplo, en redes Wi-Fi de 2.4 GHz, los canales 1, 6 y 11 son los más utilizados porque no se superponen.
2. **Ajuste de la potencia de transmisión:** Configurar una potencia demasiado alta puede causar interferencias con otros puntos de acceso, mientras que una potencia baja puede dejar zonas con señal débil.
3. **Configuración del SSID:** Es recomendable utilizar un nombre claro para identificar la red. Además, se puede configurar el SSID como visible u oculto según las necesidades de seguridad.
4. **Seguridad del punto de acceso:** Implementar protocolos como WPA3 y activar el filtrado de direcciones MAC para mayor control.
5. **Uso de frecuencias duales:** Configurar bandas de 2.4 GHz y 5 GHz permite separar dispositivos según sus capacidades y mejorar el rendimiento.

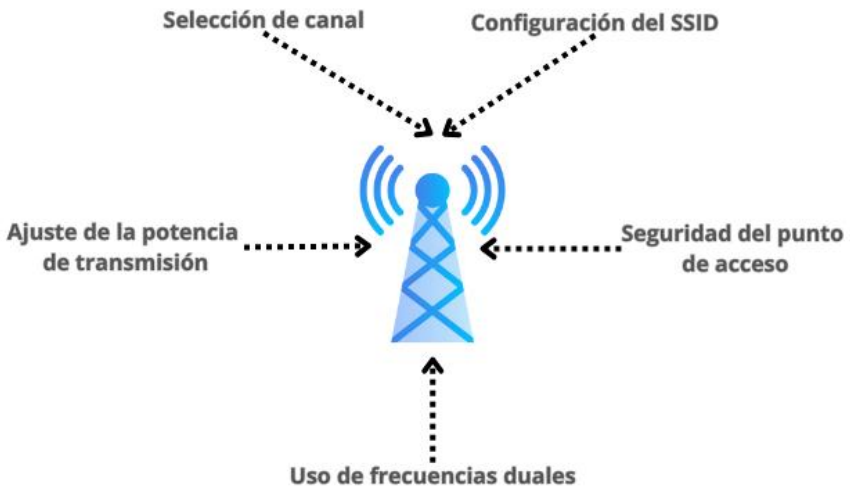

Imagen 13: Sugerencias para la configuración de un AP.
Fuente: Elaboración propia.

Routers inalámbricos

Según Tanenbaum et al. (2021) mencionan que, los routers inalámbricos son el núcleo de una red doméstica o empresarial, y su configuración adecuada es crucial, por lo tanto, los pasos básicos incluyen:

1. **Configuración del servidor DHCP:** Este servicio asigna automáticamente direcciones IP a los dispositivos conectados, facilitando la gestión de la red.
2. **Asignación de IP estática:** En algunos casos, es necesario asignar direcciones IP fijas a dispositivos críticos como servidores o cámaras de seguridad.
3. **Configuración de QoS:** La calidad de servicio permite priorizar ciertos tipos de tráfico, como videollamadas o transmisión de video, para garantizar un rendimiento fluido.
4. **Firewall y NAT:** Activar estas funciones proporciona una capa adicional de seguridad, protegiendo la red de accesos no autorizados.
5. **Actualización del firmware:** Mantener el software del router actualizado asegura que la red esté protegida contra vulnerabilidades conocidas.
6. **Creación de redes para invitados:** Configurar una red separada para invitados evita que accedan a recursos internos de la red principal.

Una configuración correcta de puntos de acceso y routers inalámbricos es fundamental para garantizar la estabilidad, seguridad y rendimiento de la red, adaptándose a las necesidades específicas de cada entorno.

Imagen 14: Sugerencias para la configuración de un router inalámbrico.
Fuente: Elaboración propia.

4.5. Sugerencias para la instalación y pruebas de funcionamiento

Instalación

Según Cisco (2020), menciona que, la instalación de una red inalámbrica incluye múltiples etapas críticas para garantizar su correcto funcionamiento:

1. **Ubicación estratégica de los puntos de acceso**: Los puntos de acceso deben instalarse en áreas donde puedan maximizar la cobertura y minimizar las interferencias. Esto incluye evitar obstáculos como paredes gruesas o equipos electrónicos que puedan bloquear la señal.
2. **Montaje adecuado:** Los puntos de acceso pueden instalarse en techos, paredes o soportes diseñados específicamente para optimizar la propagación de la señal.
3. **Conexión con PoE o fuentes externas:** Si se utiliza Power over Ethernet (PoE), esto simplifica la instalación al eliminar la necesidad de cables de alimentación adicionales, facilitando el diseño limpio y eficiente.
4. **Verificación de conexiones:** Asegurarse de que todos los puntos de acceso y routers estén correctamente conectados a la red y al sistema de gestión central, si corresponde.
5. **Seguridad física:** Proteger los dispositivos contra manipulaciones no autorizadas instalándolos en ubicaciones seguras.

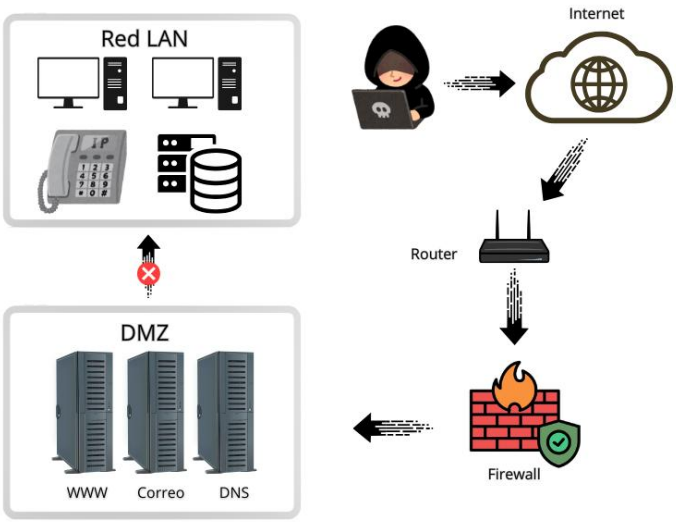

Imagen 15: Diseño de una Red Desmilitarizada.
Fuente: Elaboración propia.

Pruebas

Las pruebas de funcionamiento son esenciales para verificar que la red cumple con los objetivos de diseño:

1. **Pruebas de velocidad y latencia:** Herramientas como Speedtest, iPerf y Ping se utilizan para medir la calidad de la conexión en diferentes ubicaciones dentro del área de cobertura.
2. **Evaluación de cobertura:** Mapear las áreas de cobertura utilizando herramientas como Ekahau o HeatMapper para identificar puntos muertos o zonas con baja señal.
3. **Pruebas de carga:** Simular múltiples conexiones simultáneas para evaluar cómo la red maneja situaciones de alta demanda.
4. **Verificación de seguridad:** Realizar auditorías para asegurarse de que las configuraciones de cifrado, autenticación y acceso sean adecuadas.
5. **Pruebas de dispositivos conectados:** Comprobar que todos los dispositivos críticos (impresoras, cámaras de seguridad, teléfonos VoIP) funcionan correctamente dentro de la red.

Estas etapas de instalación y pruebas aseguran que la red inalámbrica esté completamente funcional, optimizada para su entorno y preparada para enfrentar las demandas diarias.

Imagen 16: Test de velocidad con la herramienta SpeedTest.
Fuente: Elaboración propia.

4.6. Solución de problemas comunes

Interferencias

Las interferencias son causadas por dispositivos electrónicos, otras redes inalámbricas o incluso electrodomésticos como microondas, por lo tanto, para resolver este problema se sugiere lo siguiente:

1. Cambiar el canal de la red para evitar la superposición con otras señales.
2. Reducir la potencia de transmisión de los puntos de acceso si están demasiado cerca unos de otros.
3. Utilizar frecuencias de 5 GHz, menos congestionadas que las de 2.4 GHz.

Baja velocidad

Una red puede experimentar baja velocidad debido a lo siguiente:

1. **Saturación del ancho de banda:** Limitar el acceso de dispositivos no esenciales o aplicar políticas de QoS.
2. **Problemas en el hardware:** Verificar que los puntos de acceso y routers soporten las velocidades esperadas.
3. **Obsolescencia de los dispositivos:** Sustituir equipos antiguos por versiones compatibles con estándares actuales como Wi-Fi 6.

Conexiones inestables

Las conexiones inestables pueden deberse a configuraciones incorrectas o interferencias, para solucionarlo se sugiere:

1. Actualizar el firmware de los routers y puntos de acceso.
2. Verificar la configuración de seguridad y evitar el uso de protocolos obsoletos como WEP.
3. Asegurar una instalación física adecuada, evitando obstáculos que puedan bloquear la señal.

Pérdida de conectividad

Este problema ocurre cuando los dispositivos no pueden acceder a la red, por lo tanto, se recomienda:

1. Reiniciar los puntos de acceso o routers.
2. Hay que confirmar que el servidor DHCP está asignando direcciones IP correctamente.
3. Realizar un diagnóstico para identificar cables desconectados o dañados.

Problemas de autenticación

Cuando los usuarios no pueden conectarse a la red debido a errores en la autenticación, se recomienda:

1. Verificar las credenciales de acceso y restablecer contraseñas si es necesario.
2. Configurar un servidor RADIUS para autenticación más robusta.
3. Hay que asegurar que las configuraciones de seguridad coincidan entre los dispositivos y el punto de acceso.

Un enfoque sistemático para identificar y resolver estos problemas garantiza que la red inalámbrica opere de manera eficiente y confiable.

Imagen 17: Problemas comunes en accesos inalámbricos.
Fuente: Elaboración propia.

4.7. Problemas de accesos inalámbricos

Tabla 4: Problemas de accesos inalámbricos en Empresas internacionales.

Empresa / Proyecto	**Problema Principal**	**Lecciones Clave**
Palm Inc. (2002-03, Silicon Valley)	Un ejecutivo instaló un rogue AP personal (Apple AirPort) dentro de la oficina, interrumpiendo la red corporativa durante una reunión ejecutiva.	Control y monitoreo de entornos físicos; detección temprana de redes no autorizadas (rogue AP).
Microsoft (2019-2021, interna)	Se detectaron más de 1.000 AP no autorizados en varios edificios mediante correlación de telemetría y machine learning.	Implementar WIDS/WIPS, segmentación de red, desactivación automática de puertos maliciosos.
Target (Retail, EE. UU., 2013)	Hackers entraron a la red corporativa a través de credenciales de un contratista (sistema HVAC), luego desplegaron rogue APs para exfiltrar datos de tarjetas (≈ 40M clientes).	Reforzar la autenticación; segmentar redes de terceros y supervisar todos los dispositivos conectados.
Home Depot (Retail, EE. UU., 2014)	Vulnerabilidades en la Wi-Fi corporativa permitieron acceso no autorizado, robo de datos de clientes (≈ 56M tarjetas).	Asegurar APs; usar WPA2/WPA3, segmentar redes, auditar conexiones inalámbricas.
Wendy's / Forever 21 (Retail, 2016-17)	Hackers explotaron la Wi-Fi de invitados o POS, accediendo a datos de clientes y tarjetas (≈ 18 M tarjetas en Wendy's, casos similares en Forever 21).	Políticas Wi-Fi robustas, aislamiento total de redes públicas o de invitados.
Ciberdelincuencia en estaciones UK (2024)	Un empleado manipuló el portal de Wi-Fi público en estaciones de tren, mostrando mensajes	Gestionar acceso administrativo; auditorías

	terroristas sin comprometer datos personales.	frecuentes del sistema de portal; segmentación segura.
APT28 / Fancy Bear (GRU, 2022, Washington, DC)	Hackers de inteligencia usaron una red Wi-Fi vulnerable en edificio vecino para infiltrarse sin estar físicamente presentes ("nearest neighbor attack").	Implementar WPA3, NAC/RADIUS, monitoreo continuo; asegurar redes vecinas si hay densidad urbana.

Fuente: Elaboración propia.

4.8. Caso de estudio

Una universidad enfrenta problemas de conectividad en su campus, afectando el acceso a plataformas educativas y la comunicación entre estudiantes y docentes, generando un problema que se debe a la mala ubicación de los puntos de acceso, la saturación de un solo canal Wi-Fi y la falta de segmentación del tráfico de red.

Recomendaciones para el análisis:

1. Se debe realizar un estudio de sitio utilizando herramientas como por ejemplo Ekahau Site Survey para identificar zonas con baja cobertura e interferencias.
2. Es necesario redistribuir los puntos de acceso asegurando una cobertura óptima y configurar en diferentes canales para evitar la saturación.
3. Aplicar políticas de calidad de servicio (QoS) para priorizar el tráfico académico y reducir la congestión en horas pico.
4. Aumentar la seguridad mediante la adopción de WPA3 y la segmentación del tráfico con VLANs.

Con las recomendaciones, se puede suponer que la conectividad mejora en un 40%, disminuyen las quejas de los usuarios y se optimiza el uso de los recursos de red, asegurando estabilidad y seguridad.

Preguntas para el análisis:

1. ¿Por qué la redistribución de los puntos de acceso y la asignación de distintos canales puede mejorar la conectividad en el campus?
2. ¿Cuál es la ventaja principal de implementar políticas de calidad de servicio (QoS) en una red universitaria?
3. ¿Cómo contribuye la segmentación de la red con VLANs a la seguridad y eficiencia de la conectividad?

4.9. Resumen Ejecutivo del Capítulo

El capítulo abordó las claves para diseñar e implementar redes inalámbricas eficientes y seguras, donde se explicaron aspectos fundamentales como la cobertura, capacidad y seguridad, considerando factores como obstáculos físicos, interferencias y densidad de usuarios. Se presentaron herramientas de análisis y planificación, que permiten evaluar el entorno y optimizar la ubicación de puntos de acceso, y, también se incluyen recomendaciones para configurar routers y APs, así como para su correcta instalación y prueba de funcionamiento, es necesario mencionar que se discuten problemas comunes como interferencias o caídas de señal, y se brindan soluciones prácticas.

El capítulo resalta la importancia de ajustar la potencia de transmisión, seleccionar canales adecuados y aplicar normas de seguridad, y, finalmente, se expuso un caso de estudio en una empresa de tres pisos, que enfrenta desafíos de conectividad, y se plantean estrategias para mejorar su red inalámbrica corporativa.

4.10. Evaluación del capítulo

¿Cuál es la herramienta ideal para realizar un mapeo de cobertura?

a) DHCP Analyzer
b) Ekahau Site Survey
c) Speedtest
d) QoS Configurator

¿Qué protocolo de seguridad es más recomendado actualmente?

a) WEP
b) WPA
c) WPA2
d) WPA3

¿Cuál es el estándar que mejora la capacidad de las redes inalámbricas?

a) Wi-Fi

b) Wi-Fi 5
c) Wi-Fi 6
d) Wi-Fi 3

¿Qué componente asigna direcciones IP automáticamente en una red?

a) Router
b) DHCP
c) Firewall
d) AP

¿Cuál es la principal ventaja del uso de redes Mesh?

a) Reducción de velocidad
b) Centralización de tráfico
c) Distribución de carga y cobertura
d) Costos más elevados

REFERENCIAS BIBLIOGRÁFICAS

Bellalta, B. (2016). IEEE 802.11ax: High-efficiency WLANS. IEEE Wireless Communications, 23(1), 38-46. https://doi.org/10.1109/MWC.2016.7422404

Cisco. (2020). Campus LAN and Wireless LAN Solution Design Guide. Cisco: https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-campus-lan-wlan-design-guide.html?dtid=osscdc000283

Ekahau. (2025). Ekahau. The Ultimate Wi-Fi 7 Upgrade Guide: https://www.ekahau.com/wp-content/uploads/2025/02/The-Ultimate-Wi-Fi-7-Upgrade-Guide.pdf

Kurose, J., & Ross, K. (2021). Computer Networking: A Top-Down Approach (8 th. ed.). Pearson Education Limited. ISBN: 978-1-292-40546-9

Oppenheimer, P. (2004). Top-Down Network Design (Segunda ed.). Cisco Press. ISBN: 978-1-58705-152-4

Tanenbaum, A., Wetherall, D., & Feamster, N. (2021). Computer Networks (Sexta ed.). Pearson Education Limited. ISBN: 978-1292374062

Capítulo5: Seguridad en Redes Inalámbricas

La seguridad en redes inalámbricas constituye un componente crítico para la protección de datos y la preservación de la privacidad en un entorno cada vez más interconectado. El crecimiento exponencial en el uso de redes Wi-Fi ha traído consigo un aumento proporcional en los riesgos asociados, como el acceso no autorizado, la intercepción de datos y diversos tipos de ataques cibernéticos. En este capítulo se abordan los principales desafíos en materia de seguridad inalámbrica, así como las soluciones disponibles para mitigarlos. Se destaca la relevancia de implementar protocolos robustos, realizar configuraciones adecuadas y adoptar buenas prácticas que refuercen la integridad de la red. Asimismo, se analizan los protocolos de seguridad más utilizados WEP, WPA, WPA2 y WPA3 junto con los métodos de autenticación y cifrado que permiten resguardar las comunicaciones inalámbricas. Finalmente, se ofrecen recomendaciones prácticas para fortalecer la seguridad de las redes, complementadas con un caso aplicado que permitirá consolidar los conocimientos adquiridos. (Stallings, 2015).

Objetivos:

- Identificar las principales amenazas y vulnerabilidades en redes inalámbricas.
- Comprender los protocolos de seguridad WEP, WPA, WPA2 y WPA3.
- Explicar los conceptos de autenticación y cifrado en redes inalámbricas.
- Aprender a configurar redes seguras para proteger la información.
- Establecer políticas y mejores prácticas para garantizar la seguridad en redes inalámbricas.

5.1. Principales Amenazas y Vulnerabilidades

Las redes inalámbricas presentan vulnerabilidades inherentes debido a su naturaleza, donde las principales amenazas incluyen:

- **Intercepción de Señal:** Los atacantes pueden capturar el tráfico de datos transmitido por el aire utilizando herramientas como Wireshark, de tal forma que este tipo de ataque se ve facilitado por la transmisión de datos en un medio compartido y sin barreras físicas que limiten el acceso a la señal (Lowe, 2021).
- **Acceso no Autorizado:** Usuarios no autorizados pueden conectarse a la red si no se utilizan medidas de seguridad adecuadas, como contraseñas robustas o autenticación multifactor, este acceso puede derivar en la manipulación de dispositivos, robo de información o ataques internos (Sankar et al., 2004).
- **Ataques de Hombre en el Medio (MITM):** En este tipo de ataque, un intruso intercepta y posiblemente altera la comunicación entre dos partes sin que estas lo detecten, donde los atacantes pueden redirigir el tráfico, recopilar credenciales o insertar datos maliciosos (Schneier, 2015).
- **Ataques de Fuerza Bruta:** Los atacantes intentan adivinar contraseñas mediante la prueba sistemática de combinaciones posibles, donde herramientas como Hydra o John the Ripper automatizan este proceso, lo que lo hace particularmente peligroso si se utilizan contraseñas débiles (Beard y Stallings, 2015).
- **Rogue Access Points:** También conocidos como puntos de acceso falsos, son dispositivos configurados por atacantes para imitar redes legítimas, permitiendo que los usuarios se conecten a estos puntos, exponiendo sus datos a intercepciones.
- **Denegación de Servicio (DoS):** En un ataque DoS, el atacante interrumpe la conectividad al inundar la red con tráfico malicioso, lo que puede colapsar el punto de acceso o degradar su rendimiento (IEEE, 2021).
- **Vulnerabilidades en el Hardware o Firmware:** Dispositivos de red que no se actualizan regularmente pueden contener fallos de seguridad explotables, permitiendo a los atacantes utilizar estas vulnerabilidades para obtener acceso no autorizado o para tomar el control del dispositivo (Lowe, 2021).
- **Phishing en Redes Wi-Fi Públicas:** En redes abiertas, los atacantes pueden crear páginas falsas que simulan ser

portales de autenticación para capturar credenciales de los usuarios.

- **Sniffing y Spoofing:** El sniffing implica la captura del tráfico de red, mientras que el spoofing permite a los atacantes suplantar la identidad de dispositivos o usuarios para obtener acceso no autorizado.
- **Ataques de KRACK (Key Reinstallation Attack):** Este ataque explota vulnerabilidades en el protocolo WPA2, permitiendo a los atacantes descifrar el tráfico y potencialmente modificarlo.
- **Repetidores No Autorizados:** Estos dispositivos amplifican la señal de una red legítima, pero pueden ser utilizados para interceptar o redirigir datos.

Imagen 18: Amenazas y Vulnerabilidades en el acceso inalámbrico.
Fuente: Elaboración propia.

Por lo tanto, es fundamental que los usuarios y administradores de redes sean conscientes de estas amenazas y adopten estrategias para mitigarlas, incluyendo el uso de protocolos modernos, contraseñas seguras y la educación continua sobre ciberseguridad.

5.2. Protocolos de Seguridad

WEP (Wired Equivalent Privacy)

WEP fue uno de los primeros protocolos de seguridad para redes Wi-Fi, introducido en 1997 como parte del estándar IEEE 802.11, Utiliza un cifrado basado en la clave RC4, pero su implementación con claves estáticas de 40 o 104 bits lo hace altamente vulnerable a ataques, es necesario mencionar que existen herramientas como Aircrack-ng que

permiten descifrar estas claves en pocos minutos, lo que ha llevado a su obsolescencia y a pesar de su debilidad, algunas redes antiguas todavía lo utilizan, representando un riesgo considerable (Lowe, 2021).

WPA (Wi-Fi Protected Access)

WPA fue desarrollado como una solución temporal para reemplazar a WEP mientras se trabajaba en el desarrollo de WPA2, este introduce el Protocolo Temporal de Integridad de Clave (TKIP), que genera claves únicas para cada paquete transmitido, mejorando significativamente la seguridad, sin embargo, TKIP también presenta vulnerabilidades conocidas, como el ataque de reinyección de paquetes, lo que limita su efectividad en redes modernas (IEEE, 2021).

WPA2

WPA2, introducido en 2004, es una mejora considerable sobre WPA al incorporar el Estándar de Cifrado Avanzado (AES), reconocido por su alta seguridad y resistencia a ataques, además, utiliza el Protocolo de Autenticación Extensible (EAP) para gestionar el acceso de usuarios y dispositivos, pero a pesar de su fortaleza, WPA2 es vulnerable al ataque KRACK (Key Reinstallation Attack), que explota debilidades en la implementación del protocolo de intercambio de claves (Schneier, 2015).

WPA3

Lanzado en 2018, WPA3 introduce varias mejoras importantes:

- **Autenticación Simultánea de Iguales (SAE):** Sustituye el intercambio de claves precompartidas (PSK) utilizado en WPA2, protegiendo contra ataques de diccionario y reforzando la autenticación.
- **Cifrado obligatorio:** Implementa cifrado individualizado para proteger los datos incluso en redes abiertas.
- **Protección contra fuerza bruta:** Limita la cantidad de intentos de autenticación fallidos, reduciendo la efectividad de los ataques automatizados.
- **Seguridad IoT mejorada:** Diseñado para dispositivos con capacidades limitadas, como los del Internet de las Cosas (IoT), mediante el modo Easy Connect.

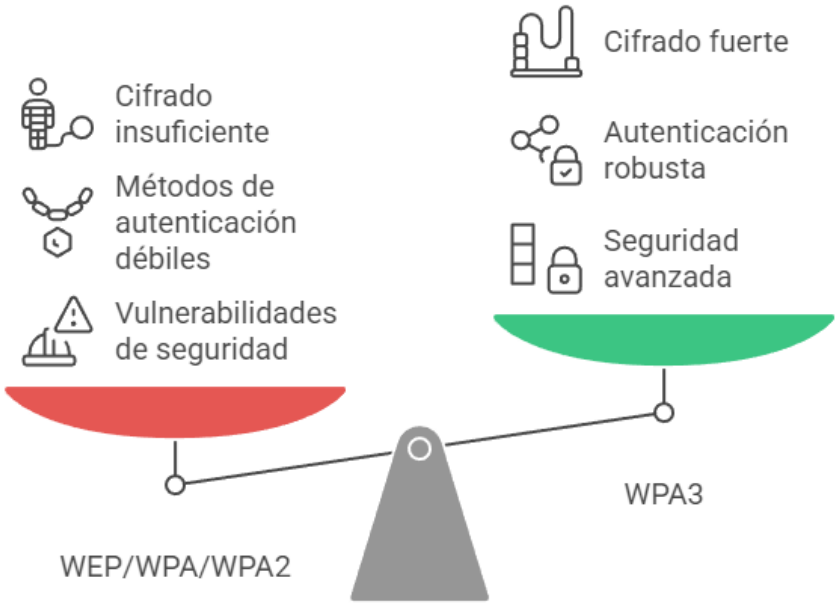

Imagen 19: Comparativa entre Protocolos de Seguridad.
Fuente: Elaboración propia.

Estas características hacen de WPA3 el protocolo de seguridad más avanzado y confiable actualmente disponible.

5.3. Autenticación y Cifrado

La autenticación y el cifrado son pilares fundamentales para garantizar la seguridad en redes inalámbricas.

Autenticación

La autenticación es el proceso de verificar la identidad de los usuarios o dispositivos que intentan acceder a una red, por lo tanto, algunos de los principales métodos de autenticación incluyen:

1. **Autenticación basada en contraseña:** Este es el método más común, pero también el más vulnerable si no se utilizan contraseñas robustas, de tal forma que se extienden algunas recomendaciones que incluyen el uso de contraseñas largas, con combinaciones de letras, números y caracteres especiales.
2. **Certificados digitales:** Proporcionan un nivel más alto de seguridad al utilizar claves criptográficas únicas para autenticar usuarios o dispositivos.
3. **Biometría:** Tecnologías como el reconocimiento facial o de huellas digitales son cada vez más utilizadas debido a su conveniencia y seguridad.
4. **Autenticación multifactor (MFA):** Combina dos o más factores, como algo que el usuario sabe (contraseña), algo que tiene (un

token físico o dispositivo móvil) y algo que es (biometría), para aumentar significativamente la seguridad.

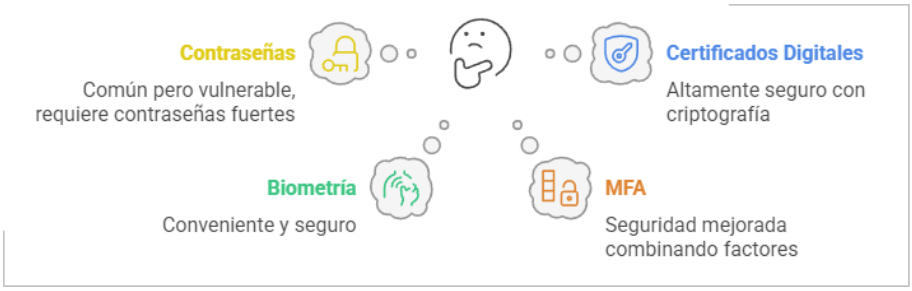

Imagen 20: Métodos de Autenticación.
Fuente: Elaboración propia.

Cifrado

El cifrado asegura que los datos transmitidos no puedan ser leídos por terceros no autorizados, por lo tanto, se especifican algunos de los algoritmos y técnicas de cifrado más utilizados son:

1. **AES (Advanced Encryption Standard):** Es el estándar más utilizado en la actualidad debido a su alta seguridad y eficiencia, ya que utiliza bloques de cifrado de 128, 192 o 256 bits para garantizar que los datos sean inaccesibles para los atacantes.
2. **TKIP (Temporal Key Integrity Protocol):** Aunque fue una mejora temporal sobre WEP, ha sido reemplazado por AES debido a sus vulnerabilidades conocidas.
3. **Cifrado de extremo a extremo (E2EE):** Garantiza que solo los usuarios finales puedan acceder a los datos, incluso si se interceptan durante la transmisión.
4. **Cifrado basado en ECC (Elliptic Curve Cryptography):** Utilizado en dispositivos IoT, proporciona alta seguridad con claves más pequeñas, lo que es ideal para dispositivos con recursos limitados.

5.4. Medidas para la configuración de redes seguras

La configuración de redes seguras implica una serie de medidas para proteger la red y los datos que se transmiten a través de ella, por tal se incluyen las siguientes medidas:

1. **Cambiar contraseñas predeterminadas:** Todos los dispositivos, como enrutadores y puntos de acceso, vienen con contraseñas predeterminadas que suelen ser conocidas o fáciles de adivinar, de tal

forma que es crucial cambiarlas inmediatamente después de la instalación.

2. **Habilitar WPA3 o el protocolo de seguridad más avanzado disponible:** WPA3 ofrece el nivel más alto de protección para redes inalámbricas, pero, si los dispositivos no son compatibles con WPA3, se recomienda al menos WPA2 con AES habilitado.
3. **Ocultar el SSID:** Aunque no garantiza una seguridad completa, ocultar el identificador de red (SSID) dificulta que usuarios no autorizados detecten la red.
4. **Filtrado de direcciones MAC:** Permite configurar el enrutador para que solo los dispositivos con direcciones MAC específicas puedan conectarse a la red.
5. **Configurar una red de invitados:** Para evitar riesgos, los usuarios externos deben conectarse a una red de invitados separada de la red principal.
6. **Implementar listas de control de acceso (ACL):** Las ACL restringen el acceso a ciertos recursos o dispositivos según direcciones IP o MAC.
7. **Actualizar periódicamente el firmware del enrutador:** Los fabricantes lanzan actualizaciones para corregir vulnerabilidades conocidas y mejorar la seguridad.
8. **Habilitar firewalls:** Un firewall integrado en el enrutador o un software de firewall en los dispositivos conectados puede prevenir accesos no autorizados y ataques externos.
9. **Configurar VPN para acceso remoto:** Las redes privadas virtuales (VPN) ofrecen un túnel cifrado para proteger las conexiones remotas y garantizar la privacidad.
10. **Monitorizar el tráfico de la red:** Utilizar herramientas de análisis de red para detectar actividades inusuales o conexiones no autorizadas.
11. **Segmentar la red:** Separar la red en diferentes segmentos o VLANs para limitar el acceso entre dispositivos.

Imagen 21: Medidas para Redes Seguras.
Fuente: Elaboración propia.

5.5. Políticas y Mejores Prácticas de Seguridad

Para garantizar la seguridad en redes inalámbricas, es esencial establecer y mantener políticas y mejores prácticas efectivas, de tal forma que se establecen algunas recomendaciones:

1. **Capacitación continua:** Educar a los usuarios y administradores sobre los riesgos actuales y las formas de mitigarlos, esto incluye talleres sobre buenas prácticas de seguridad, como el manejo de contraseñas seguras y la identificación de posibles amenazas.
2. **Creación de políticas claras:** Definir reglas y estándares para el uso de la red, por ejemplo, especificar qué dispositivos pueden conectarse, los niveles de acceso según los roles, frecuencia de los cambios de contraseñas y dividir la red en segmentos lógicos para minimizar el impacto de posibles ataques.
3. **Auditorías periódicas:** Realizar revisiones regulares de la red para identificar y corregir vulnerabilidades antes de que puedan ser explotadas.
4. **Implementación de mecanismos de respuesta a incidentes:** Establecer un protocolo claro para actuar rápidamente ante una brecha de seguridad, esto incluye, identificar la causa del incidente, contenerlo y aplicar medidas para evitar que vuelva a ocurrir.
5. **Registro y monitoreo continuo:** Utilizar sistemas de gestión de eventos y registros para monitorizar la actividad de la red, esto permite detectar comportamientos anómalos que podrían indicar un ataque.
6. **Uso de tecnología actualizada:** Garantizar que todos los dispositivos, incluidos los enrutadores y puntos de acceso, utilicen versiones de firmware y hardware actualizadas que incluyan los últimos parches de seguridad.
7. **Seguridad física de los dispositivos:** Limitar el acceso físico a los equipos críticos para evitar manipulaciones no autorizadas.
8. **Pruebas de penetración regulares:** Simular ataques para evaluar la robustez de la red y reforzar las áreas vulnerables detectadas.

Imagen 22: Estrategias comprehensivas de seguridad de redes inalámbricas.
Fuente: Elaboración propia.

5.6. Problemas de seguridad

Tabla 5: Problemas de seguridad y lecciones aprendidas en empresas Internacionales

Entorno	Institución / Empresa	Problemas principales	Lecciones clave
Educación universitaria	Universidad grande (estudio Macquarie University, Australia)	Cobertura Wi-Fi limitada en zonas del campus, señal débil y lentitud en horas pico. Se identificaron zonas muertas y congestión durante la jornada académica.	Realizar encuestas RF (site-surveys), mapas de calor, modelado de cobertura y optimización por ubicación física de APs.
Educación universitaria	Colorado, EE. UU. (Universidad de Colorado Boulder)	Cambios significativos en patrones de conectividad durante el semestre COVID-19, con gran variabilidad en densidad y flujo de usuarios.	Analizar datos dinámicos del ecosistema Wi-Fi y ajustar planificación en base a comportamiento real de usuarios.

Hospitales / Salud	Akron Children's Hospital (EE. UU.)	Calidad Wi-Fi inconsistente en áreas críticas, pérdida de paquetes, lentitud, retransmisiones frecuentes que afectaban dispositivos médicos e historiales electrónicos.	Implementación de monitoreo desde endpoint, análisis de UX, corrección de interferencias y mejoras de throughput con sensores en zonas críticas.
Hospitales / Salud	ITO Hospital (Tokio, Japón)	Conexiones Wi-Fi débiles en habitaciones y fallos de roaming entre pisos, uso de WEP inseguro y alta interferencia en zona comercial densa.	Cambiar cifrado obsoleto (WEP), planear canales adecuados, posicionamiento de antenas y mejorar roaming para dispositivos móviles médicos.
Educación / Salud (general)	Varios hospitales y campus grandes	Desafíos comunes: interferencia co-channel, obstáculos físicos, multipath, planificación pobre de RF en áreas especiales (baños, quirófanos).	Realizar análisis RF detallado, selección correcta de antenas, planificación de canales y cobertura inclusiva de zonas difíciles.
Transporte público	Network Rail – estaciones de tren (Reino Unido)	Wi-Fi público comprometido: usuarios visualizaron mensajes anti-musulmanes en la página de bienvenida; no se expusieron datos personales.	Mejorar control de cuentas administrativas, segmentación estricta de redes públicas, auditoría de acceso.

Transporte público	Autoridades regionales en EE. UU. (GRTC)	Ataques de ransomware impactaron sistemas de transporte, incluyendo conectividad y aplicaciones de gestión.	Fortalecer respuesta ante incidentes, respaldos fuera de línea, monitoreo de red crítica.
Gobierno municipal	Ciudad de Atlanta (EE. UU.)	SamSam ransomware paralizó servicios municipales y Wi-Fi en aeropuerto, generando pérdida de datos y costos millonarios ($2.7 M–9.5 M USD).	Segmentación de redes, actualización de sistemas, respuesta coordinada con agencias federales.
Gobierno nacional	Oficina de Administración de Personal (OPM), EE. UU.	Intrusión masiva por parte de atacantes chinos, con exposición de datos sensibles de personal del gobierno.	Detección de intrusiones, encriptación, monitoreo de credenciales, seguridad de sistemas heredados.
Infraestructura pública	Gobiernos provinciales (Canadá)	Al menos 20 redes comprometidas por campaña sostenida de hackers estatales, con espionaje digital contra entornos gubernamentales.	Seguridad reforzada de perímetro, segmentación entre entornos políticos y administrativos.

Fuente: Elaboración propia.

1.7. Caso de estudio

Una empresa sufrió una intrusión en su red Wi-Fi corporativa, donde el atacante logró acceder a información confidencial debido a la falta de cifrado adecuado y contraseñas débiles.

Tareas:

- Analizar las vulnerabilidades explotadas por el atacante.
- Proponer un nuevo esquema de seguridad basado en WPA3.
- Implementar autenticación multifactor para empleados.
- Desarrollar políticas internas de seguridad.

Preguntas para el análisis:

1. ¿Qué errores contribuyeron al acceso no autorizado?
2. ¿Cómo se podría haber evitado la intrusión mediante monitoreo?
3. ¿Qué ventajas tiene WPA3 frente a WPA2?
4. ¿Cómo proteger la red frente a ataques MITM?
5. ¿Qué papel juega la capacitación del personal?

1.8. Resumen Ejecutivo del Capítulo

Este capítulo exploró los principales riesgos y soluciones asociados a la seguridad en redes inalámbricas, donde se identificaron amenazas como el acceso no autorizado, ataques de denegación de servicio, suplantación de identidad, robo de datos, y se describen protocolos de seguridad fundamentales como WEP, WPA, WPA2 y WPA3, destacando la evolución hacia cifrados más robustos. Además, se analizaron mecanismos de autenticación (como claves compartidas y 802.1X) y técnicas de cifrado (AES y TKIP). Se ofrecen recomendaciones para configurar redes seguras, incluyendo el uso de contraseñas fuertes, ocultamiento de SSID, control de acceso y actualizaciones regulares del firmware. También se presentan políticas y buenas prácticas, como auditorías periódicas y educación de los usuarios, por último, se planteó un caso de estudio donde se muestra cómo una empresa refuerza su red inalámbrica frente a ataques, implementando medidas de prevención, detección y respuesta ante incidentes.

1.9. Evaluación del Capítulo

¿Cuál de los siguientes protocolos de seguridad es el más avanzado?

a) WEP
a) WPA
b) WPA2
c) WPA3

¿Qué ataque implica interceptar y alterar la comunicación entre dos partes?

a) Ataque de fuerza bruta
b) Ataque de Hombre en el Medio (MITM)
c) Rogue Access Point
d) Intercepción de señal

¿Qué mejora introduce WPA3 sobre WPA2?

a) Uso de TKIP
b) Encriptación opcional
c) Implementación de WEP
d) Autenticación Simultánea de Iguales (SAE)

¿Qué herramienta se utiliza para capturar el tráfico de datos en redes inalámbricas?

a) KRACK
b) Aircrack-ng
c) Wireshark
d) AES

¿Qué política ayuda a reducir riesgos de ataques internos?

a) Acceso libre a todos los dispositivos
b) Contraseñas simples
c) VLANs separadas
d) Uso compartido de claves

REFERENCIAS BIBLIOGRÁFICAS

Beard, C., & Stallings, W. (2015). Wireless Communication Networks and Systems (Primera ed.). Pearson. ISBN: 978-0133594171

IEEE. (2021). IEEE Approved Draft Standard for Information Technology -- Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks -- Specific Requirements - Part 11. IEEE STANDARDS ASSOCIATION: https://standards.ieee.org/ieee/802.11/10548/

Lowe, D. (2021). Networking All-in-One (Octava ed.). For Dummies. ISBN: 978-1119689010

Sankar, K., Sundaralingam, S., Miller, D., & Balinsky, A. (2004). Cisco Wireless LAN Security (Primera ed.). Cisco Press. ISBN: 978-1-58705-154-8

Schneier, B. (2015). Applied Cryptography: Protocols, Algorithms and Source Code in C (20a ed.). Wiley. ISBN: 978-1119096726

Capítulo6: Tecnologías Emergentes

El avance constante de las tecnologías inalámbricas ha impulsado el desarrollo de sistemas cada vez más rápidos, seguros y eficientes, transformando profundamente el panorama de las comunicaciones digitales. Este capítulo examina las tecnologías emergentes que están redefiniendo la conectividad global, entre las que destacan Wi-Fi 6 y Wi-Fi 7, cuyas mejoras en velocidad, capacidad y latencia prometen revolucionar la experiencia del usuario, además, se analiza el impacto de las redes Mesh, que optimizan la cobertura y estabilidad de la conexión en entornos residenciales y empresariales. Asimismo, se aborda el crecimiento exponencial del Internet de las Cosas (IoT), que está conectando dispositivos de manera innovadora en múltiples sectores. Finalmente, se presentan las tendencias prospectivas que podrían influir significativamente en la evolución del sector inalámbrico en las próximas décadas, ofreciendo una visión integral del futuro de la conectividad.

Objetivos:

- Comprender las características principales de las tecnologías Wi-Fi 6 y Wi-Fi 7.
- Analizar la aplicación de redes Mesh en diversos escenarios.
- Evaluar el impacto del Internet de las Cosas (IoT) en las redes inalámbricas.
- Identificar las ventajas y desafíos de las redes inalámbricas en entornos industriales.
- Explorar las tendencias futuras en tecnologías inalámbricas.

1.1. Wi-Fi 6 y Wi-Fi 7

Wi-Fi 6 y Wi-Fi 7 representan una evolución significativa en la conectividad inalámbrica, con mejoras diseñadas para satisfacer las crecientes demandas de dispositivos y aplicaciones avanzadas.

Wi-Fi 6 (802.11ax)

Wi-Fi 6, basado en el estándar IEEE 802.11ax, introduce mejoras significativas en eficiencia, capacidad y rendimiento en entornos densos, permitiendo una transmisión de datos más eficiente mediante

el uso de OFDMA (Orthogonal Frequency Division Multiple Access), lo que divide los canales en subcanales más pequeños para optimizar el tráfico de datos, además incorpora MU-MIMO (Multi-User Multiple Input Multiple Output) mejorado, lo que facilita la comunicación simultánea con múltiples dispositivos, aumentando la capacidad de la red sin degradar el rendimiento. A continuación, se detallan sus características clave:

- **Orthogonal Frequency Division Multiple Access (OFDMA):** Esta técnica permite que múltiples dispositivos compartan el mismo canal de transmisión dividiéndolo en subcanales, mejorando la eficiencia espectral y reduciendo la latencia en redes congestionadas (Mozaffariahrar et al., 2022).
- **Multi-User Multiple Input Multiple Output (MU-MIMO):** Wi-Fi 6 permite hasta 8 flujos espaciales simultáneos, lo que mejora la capacidad de la red y reduce la latencia al permitir que múltiples dispositivos transmitan y reciban datos al mismo tiempo (Wang et al., 2022).
- **Target Wake Time (TWT):** Introduce una programación eficiente del tiempo de activación de los dispositivos, lo que reduce el consumo energético y optimiza el uso de la batería en dispositivos IoT y móviles.
- **1024-QAM:** Este esquema de modulación cuadrática de amplitud aumenta la cantidad de datos transmitidos por símbolo, mejorando la velocidad de transmisión hasta en un 25% en comparación con Wi-Fi 5 (Tokhirov y Aliev, 2023).
- **Basic Service Set (BSS) Coloring:** Una técnica que reduce la interferencia en entornos con muchas redes Wi-Fi superpuestas, permitiendo una mayor eficiencia en el uso del espectro.
- **Mayor cobertura y estabilidad:** Wi-Fi 6 optimiza la transmisión de datos en entornos con muchos dispositivos conectados, manteniendo una calidad de servicio estable.

Imagen 23: Características de Wi-Fi 6
Fuente: Elaboración propia.

Gracias a estas innovaciones, Wi-Fi 6 ha permitido mejorar la experiencia del usuario en escenarios con alta densidad de dispositivos, como aeropuertos, estadios, oficinas y hogares con múltiples dispositivos conectados simultáneamente.

Wi-Fi 7 (802.11be)

Wi-Fi 7, basado en el estándar IEEE 802.11be, introduce aún mayores avances en velocidad y eficiencia espectral, permitiendo ofrecer anchos de banda de hasta 320 MHz, el doble que Wi-Fi 6, y utiliza la modulación 4096-QAM, que aumenta la densidad de datos transmitidos; otra innovación clave es la operación multienlace (MLO, Multi-Link Operation), que permite que los dispositivos transmitan datos simultáneamente en múltiples bandas (2.4 GHz, 5 GHz y 6 GHz), reduciendo la latencia y mejorando la confiabilidad de la conexión.

Este nuevo estándar introduce varias innovaciones clave que lo hacen ideal para aplicaciones que requieren alta velocidad y baja latencia, tales como:

- **Ancho de banda de 320 MHz:** Una de las mejoras más significativas de Wi-Fi 7 es la ampliación del ancho de banda hasta 320 MHz, lo que permite un aumento exponencial en la capacidad de transmisión de datos, esto se traduce en velocidades teóricas de hasta 30 Gbps, lo que duplica el rendimiento de Wi-Fi 6 (Chen et al., 2022).
- **16x16 Multi-User Multiple Input Multiple Output (MU-MIMO):** Wi-Fi 7 introduce una capacidad expandida de MU-MIMO, permitiendo que hasta 16 dispositivos transmitan y reciban datos simultáneamente en lugar de los 8 de Wi-Fi 6, por tal razón esto mejora drásticamente la eficiencia en entornos con muchos dispositivos conectados (Jeknić y Kocan, 2023).

- **4K-QAM (Quadrature Amplitude Modulation):** Aumenta la cantidad de datos transmitidos en cada símbolo en comparación con la modulación 1024-QAM de Wi-Fi 6, lo que mejora la eficiencia espectral y permite un mayor rendimiento en redes densamente pobladas (Murad et al., 2024).
- **Multi-Link Operation (MLO):** Esta función permite la conexión simultánea de múltiples bandas de frecuencia (2.4 GHz, 5 GHz y 6 GHz), mejorando la estabilidad de la conexión, reduciendo la latencia y optimizando el uso del espectro, es necesario indicar que esta característica es clave para aplicaciones de transmisión en tiempo real y juegos en la nube (Reshef et al., 2024).
- **Preamble Puncturing:** Permite el uso de canales parcialmente ocupados sin interferencias significativas, aumentando la eficiencia en redes congestionadas.
- **Operación en la banda de 6 GHz:** Wi-Fi 7 aprovecha plenamente la banda de 6 GHz, lo que reduce la interferencia con otros dispositivos y proporciona conexiones más estables en entornos saturados.
- **Mejoras en la calidad del servicio (QoS):** Wi-Fi 7 incorpora mejoras en la gestión del tráfico de red, garantizando una mayor priorización para aplicaciones sensibles a la latencia, como la realidad aumentada, el video en 8K y el gaming en la nube.
- **Seguridad y eficiencia energética:** Wi-Fi 7 también implementa mejoras en los protocolos de seguridad y en la eficiencia energética, lo que permite un uso más sostenible en dispositivos IoT y entornos empresariales.

Imagen 24: Desglose de las Innovaciones de Wi-Fi 7
Fuente: Elaboración propia.

Comparación entre Wi-Fi 6 y Wi-Fi 7

A continuación, se presenta una tabla comparativa que resume las principales diferencias entre ambos estándares:

Tabla 6: Comparativa Wi-Fi 6 vs Wi-Fi 7

Característica	**Wi-Fi 6 (802.11ax)**	**Wi-Fi 7 (802.11be)**
Ancho de banda máximo	160 MHz	320 MHz
Velocidad máxima	9.6 Gbps	30 Gbps
Modulación	1024-QAM	4096-QAM
MU-MIMO	8x8	16x16
Latencia	Baja	Muy baja
Multi-Link Operation	No	Sí
Operación en 6 GHz	Limitada	Total
Eficiencia energética	Alta	Mayor eficiencia
Aplicaciones clave	IoT, oficinas, hogares	AR/VR, gaming en la nube, streaming 8K

Fuente: Elaboración propia.

1.2. Redes Mesh y su Aplicación

Las redes Mesh (o redes en malla) han surgido como una solución innovadora para mejorar la conectividad en entornos donde las infraestructuras tradicionales pueden ser ineficientes o inviables, ofreciendo flexibilidad, escalabilidad y robustez en comparación con las redes inalámbricas convencionales, donde su diseño descentralizado permite que cada nodo actúe como un punto de retransmisión, optimizando el tráfico de datos y garantizando redundancia en la comunicación.

Las redes Mesh se han implementado en diversos escenarios, como el acceso a Internet en comunidades rurales, la automatización del hogar inteligente, las comunicaciones de emergencia y aplicaciones militares.

Arquitectura y Funcionamiento de las Redes Mesh

Las redes Mesh se caracterizan por su estructura descentralizada en la que cada nodo está interconectado con varios otros nodos, formando una topología de malla, permitiendo múltiples rutas para la transmisión de datos, lo que aumenta la redundancia y la estabilidad de la red, las mismas que pueden operar en distintos entornos y adoptar varias configuraciones, dependiendo de las necesidades específicas del sistema.

Tipos de Redes Mesh

- **Mesh de infraestructura:** En este modelo, algunos nodos actúan como puntos de acceso conectados a la red principal o Internet, mientras que otros nodos extienden la cobertura permitiendo la conectividad inalámbrica sin necesidad de cables adicionales (Hopjan, 2021).
- **Mesh ad hoc:** Aquí, todos los nodos pueden actuar como clientes y repetidores de señal, sin necesidad de una infraestructura preestablecida, donde dicho modelo es útil para despliegues rápidos en situaciones de emergencia o entornos con movilidad frecuente (Martín-Pascual y Andreu-Sánchez, 2023).

Componentes Principales de una Red Mesh

- **Nodos de acceso:** Son los dispositivos que proporcionan conectividad a la red.
- **Nodos de retransmisión:** Dispositivos intermedios que permiten la extensión de la señal y la distribución del tráfico de datos.
- **Puerta de enlace (Gateway):** Conectan la red Mesh a otras redes o a Internet.

Protocolos de Enrutamiento en Redes Mesh

Los protocolos de enrutamiento son esenciales en las redes Mesh, ya que determinan la mejor ruta para la transmisión de datos en un entorno dinámico, donde algunos de los protocolos más utilizados incluyen:

- **Optimized Link State Routing (OLSR):** Un protocolo basado en el estado de los enlaces que optimiza las rutas de transmisión para reducir la latencia y el consumo de ancho de banda.

- **Ad hoc On-Demand Distance Vector (AODV):** Utiliza un enfoque bajo demanda, estableciendo rutas solo cuando es necesario, lo que mejora la eficiencia energética.
- **Better Approach To Mobile Ad hoc Networking:** Divide la responsabilidad del enrutamiento entre múltiples nodos para evitar congestión y mejorar la resiliencia de la red.

Desempeño y Optimización de Redes Mesh

Para garantizar un rendimiento óptimo en redes Mesh, es fundamental abordar ciertos desafíos, como la latencia, la congestión y la interferencia, por lo tanto, se han desarrollado diversas estrategias para mejorar la eficiencia de estas redes:

- **Balanceo de carga dinámico:** Redistribuye el tráfico de datos para evitar cuellos de botella.
- **Manejo de interferencias:** Optimización del uso de canales y frecuencias para minimizar la interferencia entre nodos.
- **Optimización del consumo energético:** Implementación de estrategias de ahorro de energía en dispositivos IoT y nodos inalámbricos.

La evolución de estas estrategias ha permitido que las redes Mesh sean cada vez más eficientes y viables para aplicaciones que requieren conectividad robusta y de alta disponibilidad.

Aplicaciones de las Redes Mesh

Las redes Mesh han encontrado una amplia gama de aplicaciones en diferentes sectores debido a su adaptabilidad, resiliencia, eficiencia en la gestión de conexiones inalámbricas, y conforme a su capacidad para proporcionar cobertura extendida, alta tolerancia a fallos y una estructura descentralizada, estas redes han revolucionado diversos campos de la conectividad moderna (Son y Khoa, 2019):

- **Acceso a Internet en comunidades rurales:** Las redes Mesh se han consolidado como una solución efectiva para proporcionar conectividad en regiones rurales donde la infraestructura de telecomunicaciones es limitada o inexistente. Gracias a su estructura descentralizada, estas redes permiten el despliegue económico y escalable en áreas remotas, siendo fundamentales en escenarios como la cobertura post-desastre o zonas agrícolas (Manali y Khushboo, 2024).
- **Automatización del hogar inteligente:** Aunque los estudios más recientes se enfocan en entornos industriales o de movilidad, se reconoce que las redes Mesh continúan siendo esenciales en

sistemas de domótica. Permiten una conexión estable entre dispositivos IoT como sensores, cámaras y electrodomésticos, manteniendo una comunicación fluida sin depender de un punto central, lo cual es consistente con aplicaciones señaladas en investigaciones previas (Sujai et al., 2024).

- **Redes de emergencia y seguridad pública:** Las redes Mesh, especialmente en forma de Aerial Mesh Networks (AMNs), han sido utilizadas con éxito en entornos críticos como operaciones de rescate y gestión de desastres naturales. Estas redes permiten una rápida implementación, autoorganización y resiliencia, cualidades necesarias en entornos impredecibles (Mok Shao et al., 2024).
- **Vehicular Ad hoc Networks (VANETs):** Las redes Mesh son fundamentales para la comunicación vehicular en tiempo real. Aplicaciones VANET permiten la transmisión de información sobre tráfico, condiciones de la vía y seguridad vial. Estas redes enfrentan desafíos como seguridad, latencia y movilidad, los cuales están siendo abordados con nuevas soluciones como protocolos de autenticación ligera (Ahmed y Zakarya, 2024) y mitigación de interferencias mediante beamforming en entornos urbanos complejos (Ornelas-Gutierrez et al., 2023).
- **Aplicaciones en la industria:** Las redes inalámbricas Mesh se han consolidado como una solución clave en entornos industriales para habilitar el Internet Industrial de las Cosas (IIoT), especialmente en fábricas con sistemas de automatización y sensores distribuidos. Estas redes destacan por su capacidad de autoconfiguración, tolerancia a fallos y resiliencia, factores críticos en ambientes dinámicos y con alta interferencia.

Recientes investigaciones han demostrado avances significativos en protocolos de enrutamiento adaptativos y resilientes, diseñados para detectar y reaccionar en tiempo real ante fallos como enlaces caídos o nodos inaccesibles, mejorando la confiabilidad y disponibilidad de la red (Caleb y Thangaraj S., 2023). Además, se han propuesto mecanismos inteligentes de enrutamiento tolerante a fallos que mejoran el rendimiento del sistema IIoT, incluso ante fallos de nodos o enlaces (Kaur y Chanak, 2023).

La aplicación de redes Mesh en entornos reales ha demostrado beneficios como una mayor cobertura inalámbrica y mejor desempeño frente a obstrucciones y ruido electromagnético común en ambientes industriales (Aquino et al., 2023). Asimismo, enfoques emergentes como la autocomposición basada en inteligencia artificial y gemelos digitales están llevando la capacidad de autorrecuperación de estas redes a nuevos niveles de eficiencia y seguridad (Xinzheng et al., 2023).

Finalmente, los sistemas ciberfísicos industriales están adoptando modelos de autoorganización y colaboración entre nodos para habilitar capacidades de autorreparación, lo cual fortalece aún más la fiabilidad de estas redes en contextos industriales críticos (Piardi et al., 2024).

- **Aplicaciones en redes de telecomunicaciones:** Las redes inalámbricas Mesh se han integrado eficazmente en infraestructuras de telecomunicaciones de proveedores de servicios de Internet (ISP), especialmente en zonas urbanas densamente pobladas, como una solución para ampliar la cobertura de banda ancha sin necesidad de un despliegue masivo de cableado.

Estudios han mostrado que dichas redes permiten expandir la cobertura y a su vez mejorar la conectividad urbana, ofreciendo una alternativa eficiente y flexible a las redes cableadas tradicionales. Además, son especialmente útiles en el despliegue rápido de conectividad para zonas con limitaciones geográficas o económicas, donde otras tecnologías como la fibra óptica no son viables (Marcel Bawindsom et al., 2024).

La implementación de redes Mesh permite mejorar la capacidad de acceso a internet mediante una estructura de múltiples nodos, autoconfigurables y auto-recuperables, optimizando el uso del espectro disponible y reduciendo la necesidad de infraestructura física compleja (Neema et al., 2023). Estas redes han demostrado ser efectivas también para soportar servicios de streaming de alta demanda en entornos urbanos complejos.

Finalmente, se ha evidenciado que las redes Mesh, cuando se combinan con tecnologías como SDN (Software Defined Networking), pueden ofrecer soluciones escalables y de bajo costo para la provisión de Internet en entornos urbanos, mejorando la eficiencia del control del tráfico y reduciendo la latencia de red (Venegas Lorenti et al., 2024).

- **Eventos masivos y espacios públicos:** Se implementan en conciertos, estadios y grandes convenciones para garantizar la conectividad de los asistentes sin saturar las redes tradicionales, y gracias a su escalabilidad, permiten gestionar grandes volúmenes de usuarios de manera eficiente.

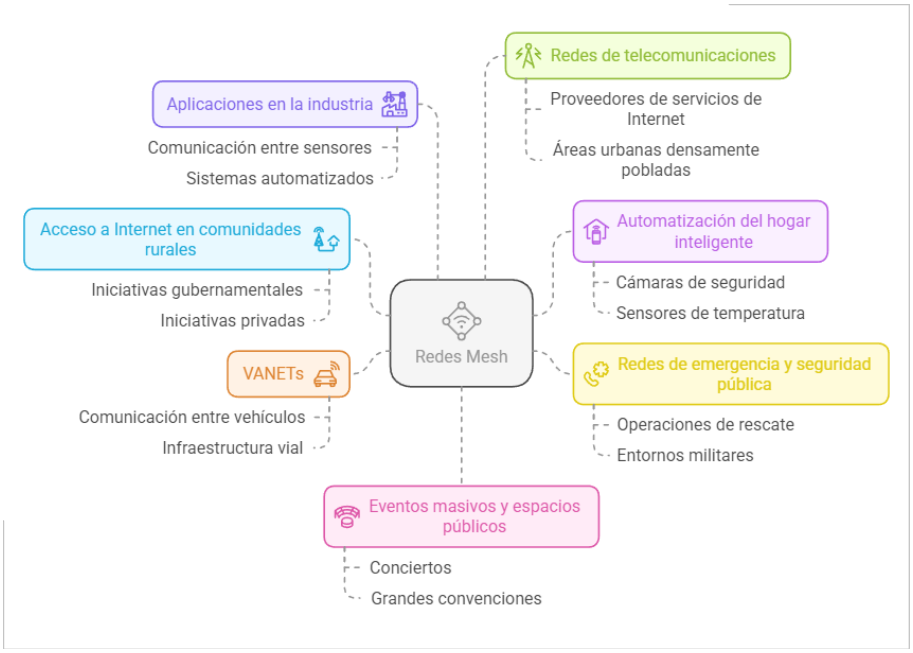

Imagen 25: Redes Mesh y sus aplicaciones.
Fuente: Elaboración propia.

El crecimiento de las redes Mesh sigue en aumento, con avances tecnológicos que mejoran su desempeño en términos de velocidad, latencia y seguridad, la misma que genera una versatilidad que las convierte en una tecnología clave para el futuro de las comunicaciones inalámbricas en múltiples sectores.

Ventajas y Desafíos de las Redes Mesh

Las redes Mesh han ganado popularidad gracias a sus múltiples ventajas, que incluyen alta redundancia, facilidad de implementación y cobertura ampliada, sin embargo, también presentan desafíos técnicos y operativos que deben abordarse para maximizar su eficiencia y seguridad.

Ventajas

- **Alta redundancia y tolerancia a fallos:** Si un nodo de la red falla, la comunicación se redirige automáticamente a través de otros nodos disponibles, lo que mejora la confiabilidad de la red.
- **Cobertura extendida y escalabilidad:** Se pueden agregar más nodos sin afectar negativamente la estabilidad de la red, lo que permite una expansión fluida y económica.
- **Reducción de costos de infraestructura:** Al eliminar la necesidad de múltiples puntos de acceso cableados, las redes

Mesh reducen significativamente los costos de instalación y mantenimiento.

- **Autoconfiguración y autogestión:** Gracias a sus protocolos dinámicos de enrutamiento, estas redes pueden adaptarse a cambios en el entorno sin intervención manual.
- **Bajo impacto ambiental:** Al optimizar el uso de la energía y reducir la necesidad de cableado, las redes Mesh pueden ser una solución más sostenible en comparación con otras tecnologías de red.

Desafíos

- **Latencia y eficiencia energética:** A medida que aumenta la cantidad de nodos y saltos en la red, la latencia puede volverse un problema, afectando el rendimiento de aplicaciones en tiempo real como videollamadas y gaming en la nube.
- **Interferencia en la red:** La proximidad de múltiples nodos puede generar congestión e interferencias en el espectro radioeléctrico, afectando la calidad de la conexión.
- **Seguridad y privacidad:** La descentralización de la red la hace más vulnerable a ataques, requiriendo el uso de protocolos de cifrado y autenticación avanzada para prevenir intrusiones.
- **Gestión del tráfico de datos:** En redes de gran escala, la distribución equitativa del tráfico y la priorización de paquetes críticos pueden representar un desafío operativo.
- **Consumo de recursos en dispositivos móviles:** Aunque la eficiencia energética ha mejorado con el tiempo, los dispositivos conectados a redes Mesh pueden experimentar un consumo de batería superior al esperado.

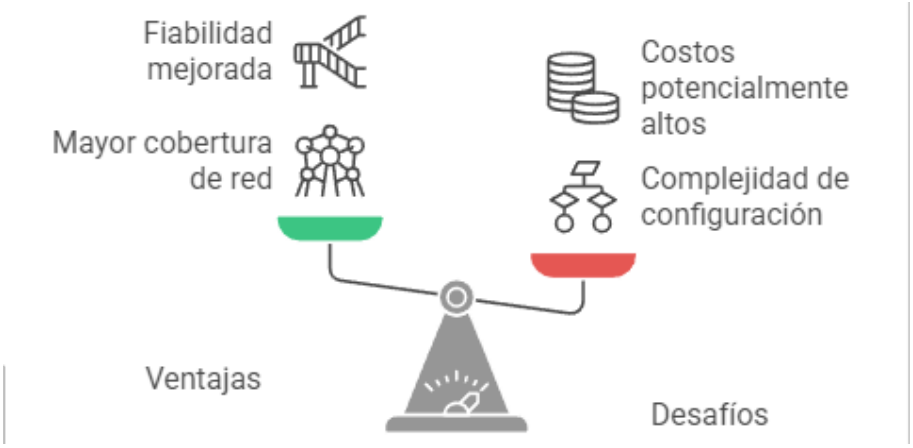

Imagen 26: Midiendo las Ventajas vs los desafíos de las Redes Mesh
Fuente: Elaboración propia.

Para abordar estos desafíos, se han desarrollado tecnologías emergentes como la inteligencia artificial aplicada al balanceo de carga, el uso de bandas de frecuencia más eficientes y mejoras en los algoritmos de enrutamiento para optimizar la distribución del tráfico.

1.3. Internet de las Cosas (IoT) y las Redes Inalámbricas

El Internet de las Cosas (IoT) continúa consolidándose como una tecnología fundamental, con aplicaciones que van desde el hogar inteligente hasta la gestión de ciudades y sectores industriales. Su integración con redes inalámbricas ha permitido la interconexión masiva de dispositivos, posibilitando la automatización y el intercambio de datos sin intervención humana (Haq Hashmi et al., 2024), (Das et al., 2023).

El IoT puede entenderse como un ecosistema compuesto por dispositivos físicos interconectados como los sensores, actuadores, dispositivos portátiles, electrodomésticos inteligentes, sistemas industriales y vehículos que recopilan, procesan y transmiten datos a través de redes inalámbricas. Su capacidad para optimizar procesos, mejorar la eficiencia y permitir la automatización ha impulsado su adopción en múltiples sectores, incluyendo la agricultura, salud, transporte y manufactura (Rodríguez-Mejía et al., 2024).

Las redes inalámbricas proporcionan la infraestructura esencial para el funcionamiento del IoT, permitiendo la conectividad sin necesidad de cableado. Existen múltiples tecnologías inalámbricas con características específicas:

- **Wi-Fi (Wireless Fidelity):** Tecnología ampliamente utilizada en entornos domésticos y comerciales para conectar múltiples dispositivos a Internet con velocidades elevadas y baja latencia.
- **Bluetooth Low Energy (BLE):** Utilizado en dispositivos de baja potencia, como wearables, sensores y sistemas de salud, debido a su bajo consumo energético y corto alcance.
- **LoRaWAN (Long Range Wide Area Network):** Ideal para áreas rurales, agrícolas e industriales por su largo alcance y eficiencia energética. Aplicaciones como la gestión de agua y maquinaria en construcción ya lo están implementando exitosamente (Enas F. et al., 2025), (Deepesh et al., 2023).
- **ZigBee:** Utilizada en redes de sensores con baja demanda energética y alta eficiencia en transmisión de datos, donde nuevas investigaciones también exploran su interoperabilidad con tecnologías como LoRa (Wang et al., 2023).
- **5G y Redes Celulares:** Permiten conexiones IoT de alta velocidad y baja latencia, facilitando la comunicación en tiempo

real para aplicaciones críticas como vehículos autónomos, telemedicina e infraestructura inteligente.

- **Redes LPWAN (Low Power Wide Area Network):** Diseñadas para dispositivos IoT que requieren conectividad de largo alcance con bajo consumo de energía, como Sigfox y NB-IoT.

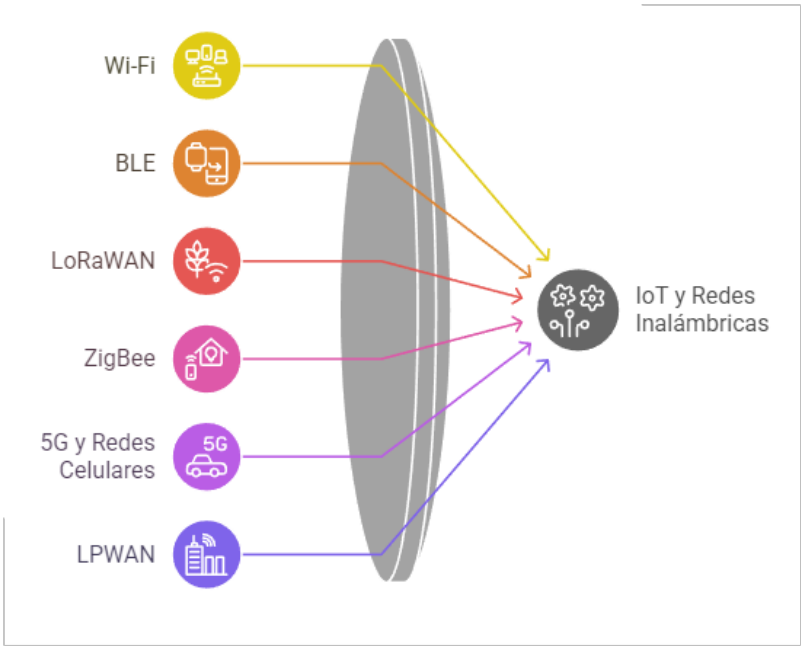

Imagen 27: El IoT y las Redes Inalámbricas.
Fuente: Elaboración propia.

Estas tecnologías, combinadas con avances en inteligencia artificial y computación en la nube, están permitiendo la integración de IoT en cada vez más aspectos de la vida cotidiana y la industria, impulsando la eficiencia y la conectividad global.

Aplicaciones del IoT en Redes Inalámbricas

La integración de IoT con redes inalámbricas ha impulsado numerosas aplicaciones en diversos sectores, transformando la manera en que las personas y las organizaciones interactúan con la tecnología (Hassan et al., 2024):

- **Ciudades inteligentes:** IoT desempeña un papel crucial en la gestión del tráfico, alumbrado público, monitoreo ambiental y gestión de residuos, dado que los sensores conectados y redes inalámbricas permiten recopilar y analizar datos en tiempo real para mejorar la eficiencia operativa y la sostenibilidad urbana, por ejemplo, incluyen sistemas de semáforos inteligentes y monitoreo de la calidad del aire.

- **Salud y bienestar:** La telemedicina y los dispositivos médicos conectados han revolucionado la atención médica, la implementación de sensores portátiles permiten monitorear constantes vitales en pacientes crónicos, alertando a los profesionales de la salud ante anomalías, además, IoT facilita la gestión de hospitales, optimizando el uso de equipos médicos y camas disponibles (Čolaković et al., 2021).
- **Industria 4.0:** La automatización industrial mediante IoT permite mejorar la eficiencia y la seguridad en entornos fabriles, donde dispositivos conectados monitorean maquinaria en tiempo real, permitiendo el mantenimiento predictivo para reducir fallas y tiempos de inactividad.
- **Hogares inteligentes:** La domótica ha crecido exponencialmente con la adopción de IoT, integrando dispositivos como asistentes de voz, termostatos inteligentes y sistemas de seguridad conectados permiten una mayor comodidad y ahorro energético en los hogares.
- **Vehículos conectados y movilidad inteligente:** IoT ha permitido la comunicación entre automóviles y la infraestructura vial para mejorar la seguridad y eficiencia del tráfico. Los vehículos autónomos y las aplicaciones de navegación en tiempo real dependen de redes inalámbricas avanzadas para optimizar rutas y reducir el tiempo de viaje.
- **Agricultura de precisión:** IoT en la agricultura permite un monitoreo detallado de cultivos y ganado mediante sensores de humedad, temperatura y calidad del suelo, permitiendo la optimización del uso de agua y fertilizantes, aumentando la productividad y reduciendo costos operativos.
- **Redes de energía inteligentes (Smart Grid):** La integración de IoT con redes eléctricas permite mejorar la distribución de energía, detectar fallas y optimizar el consumo, donde los contadores inteligentes facilitan la gestión del consumo eléctrico en tiempo real, permitiendo tarifas dinámicas y mayor eficiencia energética.
- **Seguridad y defensa:** IoT se ha implementado en sistemas de videovigilancia, drones de seguridad y sensores de detección de intrusos, como por ejemplo en el ámbito militar, se utiliza para mejorar la comunicación y la recopilación de datos en tiempo real en zonas de conflicto.

Imagen 28: Transformación Global a través de IoT y Conectividad Inalámbrica
Fuente: Elaboración propia.

Estas aplicaciones están transformando sectores clave de la economía y la vida cotidiana, impulsando una conectividad más eficiente y facilitando la toma de decisiones basada en datos.

Desafíos del IoT en Redes Inalámbricas

A pesar de sus múltiples beneficios, la implementación del IoT en redes inalámbricas presenta diversos desafíos técnicos, de seguridad y operativos que deben ser abordados para garantizar su correcto funcionamiento y sostenibilidad en el tiempo (Celik et al., 2023):

- **Seguridad y privacidad:** La creciente cantidad de dispositivos conectados representa un desafío en términos de ciberseguridad, de tal forma que los ataques como el secuestro de dispositivos, el robo de datos y las vulnerabilidades en el firmware pueden comprometer infraestructuras críticas, por lo tanto, se requiere la implementación de cifrado avanzado, autenticación multifactor y segmentación de redes para reducir riesgos (Hassan et al., 2024).
- **Gestión del tráfico de datos y congestión de la red:** El crecimiento acelerado de dispositivos IoT genera una carga significativa en las redes inalámbricas, causando congestión, latencia y pérdida de datos. Para enfrentar esto, tecnologías como Edge Computing, 5G, y computación en el borde basada en IA han demostrado reducir la latencia y mejorar la eficiencia

en la transmisión de datos (Ali et al., 2024), (Qudus et al., 2025), (Mohan y Panda, 2024).

Además, soluciones específicas como el control inteligente de la tasa de datos en protocolos como ZigBee también han sido eficaces para prevenir congestión en redes de transporte inteligentes (He et al., 2023).

- **Consumo energético y sostenibilidad:** Muchos dispositivos IoT operan con baterías, lo que limita su autonomía. Se ha avanzado en el uso de recolección de energía (energy harvesting) junto con tecnologías de bajo consumo como ZigBee, LoRaWAN, y NB-IoT para mejorar la sostenibilidad energética (Hesam Nejati et al., 2024), (Hadjur et al., 2024).

También se ha demostrado que estrategias como la transferencia cruzada de datos entre interfaces ZigBee y LoRa mejoran la eficiencia de ancho de banda y reducen el consumo energético en redes autoalimentadas (Hua et al., 2024).

- **Interoperabilidad y estandarización:** La diversidad de fabricantes y la falta de protocolos de comunicación unificados dificultan la integración de dispositivos IoT en redes heterogéneas, este percance ha generado que se tome más importancia en este asunto por parte de organizaciones como IEEE e IETF han trabajado en estándares como MQTT, CoAP y OPC-UA para mejorar la compatibilidad entre dispositivos y sistemas de distintas marcas (Patil y Banerjee, 2023).
- **Latencia y confiabilidad en aplicaciones críticas:** En contextos como la salud, manufactura y transporte, una transmisión con baja latencia y alta confiabilidad es esencial. Tecnologías como Time-Sensitive Networking (TSN) y la computación en el borde han sido integradas con éxito para garantizar estos requisitos, incluso en condiciones de red congestionadas (Gomez et al., 2023), (Avila-Campos et al., 2023).

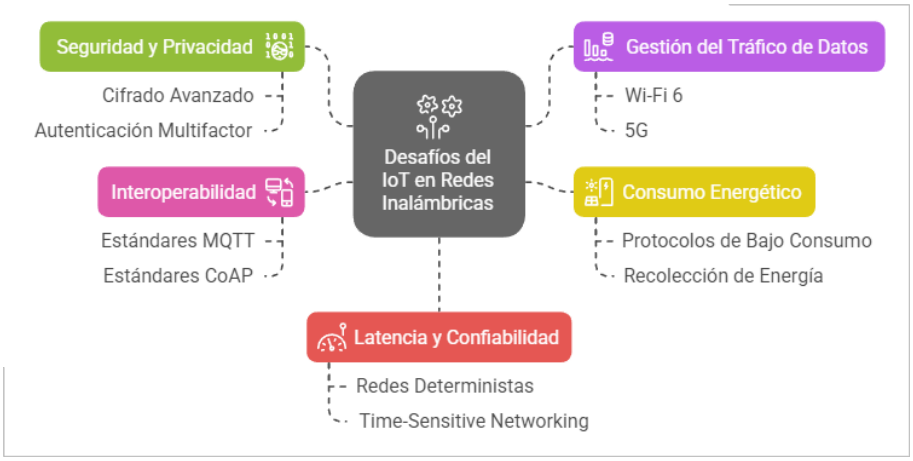

Imagen 29: Desafíos del IoT en Redes Inalámbricas

Fuente: Elaboración propia.

1.4. Tendencias Futuras

Las redes inalámbricas han experimentado una evolución acelerada en las últimas décadas, impulsadas por la creciente demanda de conectividad, el desarrollo de nuevas tecnologías y la necesidad de infraestructuras de comunicación más eficientes y sostenibles. Con la llegada del Internet de las Cosas (IoT), la inteligencia artificial (IA) y las redes 5G y 6G, las redes inalámbricas se están adaptando para manejar un volumen de dispositivos sin precedentes, al tiempo que buscan mejorar la seguridad, reducir la latencia y aumentar la eficiencia energética (Dandekar et al., 2024).

Expansión de las Redes 5G y Desarrollo de 6G

Las redes 5G han revolucionado las telecomunicaciones con su capacidad de ofrecer velocidades ultra rápidas, mayor capacidad de conexión simultánea y latencias mínimas, sin embargo, el desarrollo de 6G está en marcha, con el objetivo de llevar la conectividad a un nivel completamente nuevo, incluyendo:

- Velocidades de transmisión de datos ultra rápidas, superando los terabits por segundo.
- Latencia ultrabaja, con tiempos de respuesta en el rango de los microsegundos.
- Integración de IA, para optimizar la gestión del espectro y mejorar la seguridad.
- Uso de frecuencias terahercios (THz), permitiendo una mayor capacidad de transmisión.

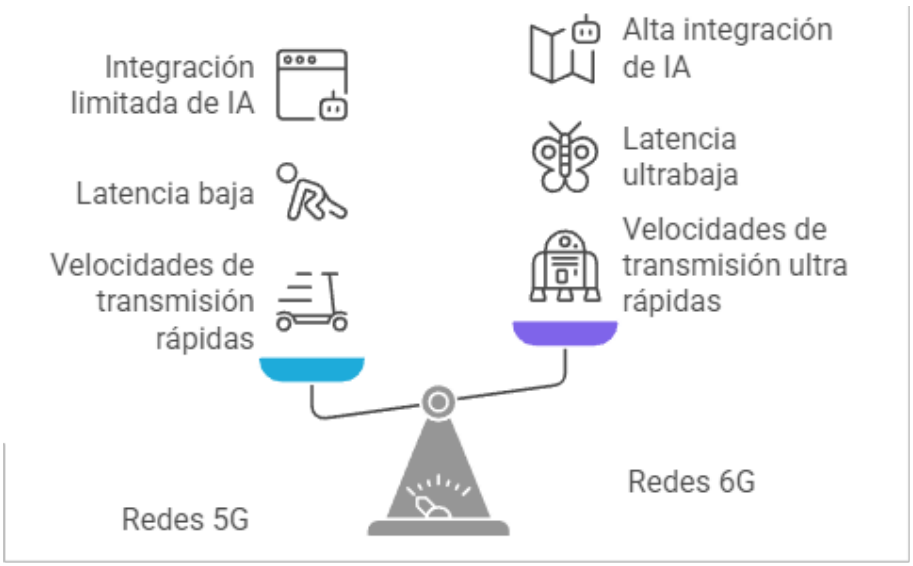

Imagen 30: Capacidades de 5G vs 6G

Fuente: Elaboración propia.

Redes Definidas por Software (SDN) y Virtualización de Redes

La virtualización de redes y las redes definidas por software (SDN) están revolucionando la gestión de infraestructuras inalámbricas al permitir un control más dinámico y eficiente de los recursos de red, donde estas tecnologías separan el plano de control del plano de datos, lo que facilita una administración más flexible y escalable de la red, optimizando su rendimiento y capacidad de adaptación a nuevas demandas (Kim, 2023).

Características clave de SDN y Virtualización de Redes:

- **Centralización del control:** SDN permite gestionar toda la red de forma centralizada a través de controladores de software, lo que facilita la optimización del tráfico y la implementación de políticas de seguridad.
- **Automatización y gestión dinámica:** La posibilidad de automatizar la configuración y administración de la red reduce costos operativos y mejora la eficiencia.
- **Segmentación de red y seguridad mejorada:** La virtualización de redes permite segmentar el tráfico y aplicar reglas de seguridad específicas por aplicación o usuario, reduciendo vulnerabilidades.
- **Optimización del uso del espectro:** Permite una mejor asignación de recursos en redes inalámbricas, aumentando la eficiencia en entornos densos y altamente dinámicos.

Aplicaciones de SDN en Redes Inalámbricas:

- **Redes empresariales:** Facilita la gestión de redes de gran escala, como en campus universitarios y corporaciones multinacionales.
- **Infraestructura en la nube:** Optimiza la conectividad entre centros de datos, asegurando alta disponibilidad y escalabilidad.
- **Redes 5G y 6G:** SDN es un pilar clave en la arquitectura de estas redes de próxima generación, permitiendo un uso más eficiente del espectro y una conectividad más robusta.
- **IoT y Smart Cities:** Ayuda a gestionar eficientemente el tráfico de datos generado por miles de dispositivos IoT en ciudades inteligentes.

Imagen 31: SDN y la Virtualización de redes
Fuente: Elaboración propia.

El impacto de SDN y la virtualización de redes seguirá creciendo en el futuro, siendo un componente esencial para la evolución de las telecomunicaciones y la optimización de infraestructuras inalámbricas en múltiples sectores.

Uso de Inteligencia Artificial y Machine Learning en Redes Inalámbricas

Las técnicas de inteligencia artificial (IA) y aprendizaje automático (ML) están siendo adoptadas en redes inalámbricas para optimizar la administración del espectro, predecir fallos y mejorar la eficiencia de transmisión de datos. Algunas de sus aplicaciones clave incluyen:

- Optimización del tráfico de datos mediante modelos predictivos.
- Mejora en la detección de intrusos y ciberseguridad.
- Mantenimiento predictivo, reduciendo tiempos de inactividad en infraestructuras de telecomunicaciones.

Redes de Baja Potencia y Sensores Inteligentes

El crecimiento del IoT ha impulsado el desarrollo de tecnologías de comunicación de baja potencia, como:

- Redes LPWAN (Low Power Wide Area Network), que permiten la conexión de dispositivos con un consumo energético mínimo.
- Sensores autónomos, capaces de operar durante años sin necesidad de recarga de baterías.
- Energía cosechada del ambiente, reduciendo la dependencia de baterías.

Seguridad y Ciberseguridad en Redes Inalámbricas

A medida que aumentan los dispositivos conectados, también crecen las amenazas de ciberseguridad, donde las futuras redes inalámbricas deberán implementar nuevas estrategias para garantizar la seguridad de la información, como:

- Uso de blockchain para autenticación descentralizada.
- Protocolos de cifrado más robustos.
- Políticas para el manejo de los dispositivos físicos.
- Inteligencia artificial aplicada a la detección de intrusos.

Redes Satelitales para Cobertura Global

El desarrollo de redes de comunicación satelital permitirá expandir la conectividad a regiones remotas y garantizar la cobertura en cualquier parte del mundo, y a medida que crece la demanda de conectividad global, las tecnologías satelitales están evolucionando para ofrecer soluciones más eficientes, de menor latencia y mayor ancho de banda.

Principales proyectos de redes satelitales:

- **Starlink (SpaceX):** Desarrollado por SpaceX, esta red de satélites LEO (Satélites de Orbita Baja) proporciona Internet de alta velocidad a nivel global, con un enfoque en áreas rurales y remotas.
- **OneWeb:** Empresa que opera una constelación de satélites LEO con el objetivo de brindar conectividad en zonas sin acceso a infraestructura terrestre.
- **Amazon Kuiper:** Proyecto de Amazon para desplegar una red de satélites LEO con el fin de proporcionar Internet de banda ancha a regiones desatendidas.
- **Telesat Lightspeed:** Una red planificada de satélites MEO para ofrecer conectividad de alta velocidad y baja latencia a clientes comerciales y gubernamentales.

Beneficios y Desafíos de las Redes Satelitales

Beneficios:

- **Cobertura global:** Capacidad de conectar cualquier punto del planeta, incluyendo áreas rurales y marítimas.
- **Baja latencia en satélites LEO:** Mejora la experiencia en aplicaciones como videollamadas y gaming en línea.
- **Resiliencia y redundancia:** Reducción de interrupciones en el servicio gracias a la interconexión de múltiples satélites.

- **Soporte para IoT y redes 6G:** Facilita la conectividad de dispositivos IoT en ubicaciones remotas y permitirá el desarrollo de redes 6G con infraestructura satelital.

Desafíos:

- **Altos costos de lanzamiento y mantenimiento:** El despliegue de satélites es costoso y requiere infraestructura avanzada.
- **Gestión de la congestión orbital y desechos espaciales:** Con miles de satélites en órbita, es necesario implementar estrategias para evitar colisiones y la acumulación de desechos espaciales.
- **Interferencia con redes terrestres:** Se deben desarrollar mecanismos para mitigar la interferencia con redes de telecomunicaciones terrestres.

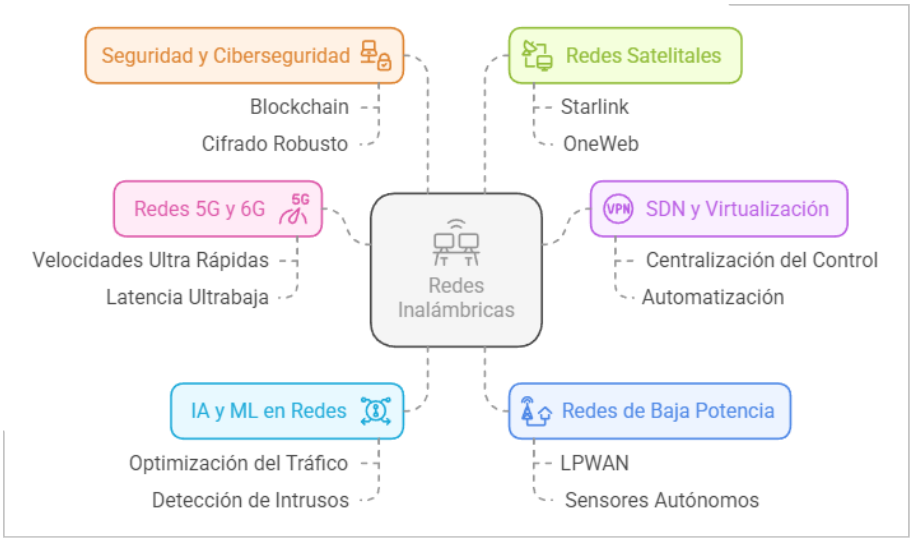

Imagen 32: Evolución y Tendencias Futuras en Redes Inalámbricas.
Fuente: Elaboración propia.

1.5. Caso de estudio

Una universidad con 10 edificios experimentaba graves problemas de conectividad, lo que afectaba significativamente la enseñanza digital y el acceso a plataformas educativas en línea. Antes de la implementación de una red Mesh, muchas aulas y oficinas administrativas sufrían de cobertura deficiente, altas tasas de latencia y congestión en las horas pico, y la incapacidad de soportar la creciente demanda de dispositivos conectados simultáneamente generaba interrupciones en las clases virtuales y dificultades en la comunicación interna entre los diferentes departamentos académicos.

Preguntas para el análisis:

1. ¿Qué propuesta plantearía usted, para la solución a la problemática? ¿Por qué?
2. ¿Qué beneficios se generarían con base a la solución planteada?
3. ¿Qué desafíos se generan en la solución a la propuesta?
4. Dado que la red Mesh proporciona redundancia automática, ¿Cómo debería configurarse la administración del tráfico en caso de que un nodo falle?
5. Uno de los edificios más alejados del campus aún presenta problemas de conexión a pesar de la implementación de la red Mesh. ¿Cuál sería la mejor estrategia para optimizar su conectividad?

1.6. Resumen Ejecutivo del Capítulo

El capítulo analizó las tecnologías inalámbricas emergentes que están transformando la conectividad moderna, destacando Wi-Fi 6 y Wi-Fi 7, con mejoras en velocidad, eficiencia espectral, baja latencia y capacidad de conexión simultánea. Se introduce el concepto de redes Mesh, que permiten ampliar la cobertura mediante nodos interconectados, ideal para entornos complejos y grandes superficies, y asimismo, se aborda la integración del Internet de las Cosas (IoT), detallando cómo los dispositivos inteligentes se comunican mediante estándares como Zigbee y LoRaWAN. Se exploran también las tendencias futuras, como la conectividad 6G, redes ultradensas, inteligencia artificial en la gestión de redes, y redes definidas por software (SDN). El capítulo concluye con un caso de estudio sobre una ciudad inteligente que implementa estas tecnologías para optimizar transporte, seguridad y servicios públicos mediante conectividad inalámbrica avanzada.

1.7. Evaluación del capítulo

¿Cuál es la principal ventaja de Wi-Fi 7 sobre Wi-Fi 6?

a) Mayor número de dispositivos soportados.
b) Mayor velocidad y menor latencia.
c) Uso de tecnología OFDMA.
d) Mejor compatibilidad con Zigbee.

¿Qué característica principal define a las redes Mesh?

a) Uso de anchos de banda superiores.
b) Conexión basada en un único nodo central.
c) Interconexión de múltiples nodos para una cobertura uniforme.
d) Optimización del uso de energía en dispositivos IoT.

¿Cuál es el principal desafío del IoT en redes inalámbricas?

a) Incrementar la velocidad de transferencia.
b) Garantizar la seguridad y privacidad de los datos.
c) Reducir el consumo de energía de los dispositivos.
d) Mejorar la cobertura en zonas rurales.

¿Cuál de las siguientes es una tendencia futura en tecnologías inalámbricas?

a) Uso exclusivo de Wi-Fi en redes industriales.
b) Redes cuánticas para mejorar la seguridad.
c) Eliminación de dispositivos IoT.
d) Dependencia total de redes Mesh.

¿Qué estándar corresponde a Wi-Fi 6?

a) 802.11ac
b) 802.11n
c) 802.11ax
d) 802.11a

REFERENCIAS BIBLIOGRÁFICAS

Ahmed, B., & Zakarya, B. (2024). ANEL: a novel efficient and lightweight authentication scheme for enhancing security in Vehicular Ad Hoc Networks (VANETs) using elliptic curve cryptography. STUDIES IN ENGINEERING AND EXACT SCIENCES, 5(2), 1-29. https://doi.org/https://doi.org/10.54021/seesv5n2-334

Ali, M., Khan, H., Afzal Rana, M. T., Ali, A., Muhammad Zeeshan, B., Rehman, S., & Alsaawy, Y. (2024). A Machine Learning Approach to Reduce Latency in Edge Computing for IoT Devices. Engineering, Technology & Applied Science Research, 14(5), 16751–16756. https://doi.org/10.48084/etasr.8365

Aquino, C., Braga, M., Carvalho, V., Moura, E., Oliveira, Y., & Gomes, R. (2023). Proceedings of the 12th Latin-American Symposium on Dependable and Secure Computing. Using IoT Mesh Networks to Extend Wireless Coverage in Industrial Environments, (págs. 204–207). https://doi.org/10.1145/3615366.3625073

Avila-Campos, P., Haxhibeqiri, J., Girmay, M., Moerman, I., & Hoebeke, J. (2023). 2023 19th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob). Residual Service Time Optimization for legacy Wireless-TSN end nodes (págs. 466-471). IEEE. https://doi.org/10.1109/WiMob58348.2023.10187722

Caleb, S., & Thangaraj S., J. (2023). 2023 International Conference on Data Science, Agents & Artificial Intelligence (ICDSAAI). Enhancing Fault Tolerance in Wireless Mesh Networks through Adaptive and Resilient Routing Protocols, (págs. 1-6). https://doi.org/10.1109/ICDSAAI59313.2023.10452547

Celik, A., Romdhane, I., Kaddoum, G., & Eltawil, A. (2023). A Top-Down Survey on Optical Wireless Communications for the Internet of Things. IEEE Communications Surveys & Tutorials, 25(1), 1-45. https://doi.org/10.1109/COMST.2022.3220504

Chen, C., Chen, X., Das, D., Akhmetov, D., & Cordeiro, C. (2022). Overview and Performance Evaluation of Wi-Fi 7. IEEE Communications Standards Magazine, 6(2), 12-18. https://doi.org/10.1109/MCOMSTD.0001.2100082

Čolaković, A., Džubur, A., & Karahodža, B. (2021). Wireless communication technologies for the Internet of Things. Science, Engineering and Technology, 1(1), 1-14. https://doi.org/10.54327/set2021/v1.i1.3

Dandekar, P., Dandekar, M., & Phutane, P. (2024). A Comprehensive Review on Wireless Communication and Networking Advances. 2024 IEEE 3rd International Conference on Electrical Power and Energy Systems-

ICEPES, (págs. 1-4). https://doi.org/10.1109/ICEPES60647.2024.10653526

Das, L., Raman Chandan, R., Kaur, P., Singh, A., Rana, A., & Shivhare, B. D. (2023). 2023 6th International Conference on Contemporary Computing and Informatics (IC3I). Advancements in Wireless Network Technologies for Enabling the (IoT): A Comprehensive Review, 6, págs. 807-814. https://doi.org/10.1109/IC3I59117.2023.10397952

Deepesh, A., Deepak, S., & KVV, R. (2023). Construction Machinery Monitoring System using LoRa WAN. International Journal For Multidisciplinary Research, 5(2). https://doi.org/10.36948/ijfmr.2023.v05i05.6326

Dhandapani, S. (2019). IMPROVISATION OF MESH NETWORK WITH WIDEBAND CODE DIVISION MULTIPLE ACCESS. IRO Journal on Sustainable Wireless Systems, 1(3), 198-205. https://doi.org/10.36548/jsws.2019.3.006

Enas F., K., Atheer M., A., Mohammad M., A. m., & Sherali, Z. (2025). LoRaWAN-based smart water management IoT applications: a review. Journal of Information and Telecommunication, 1-27. https://doi.org/10.1080/24751839.2025.2458889

Gomez, D. L., Montoya, G. A., Lozano-Garzon, C., & Donoso, Y. (2023). Strategies for Assuring Low Latency, Scalability and Interoperability in Edge Computing and TSN Networks for Critical IIoT Services. IEEE Access, 11, 42546-42577. https://doi.org/10.1109/ACCESS.2023.3268223

Hadjur, H., Ammar, D., & LefèVre, L. (2024). 2024 IEEE International Conferences on Internet of Things (iThings) and IEEE Green Computing & Communications (GreenCom) and IEEE Cyber, Physical & Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics. Deep Reinforcement Learning for Energy-efficient Selection of Embedded Services at the Edge (págs. 67-74). IEEE. https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData-Cybermatics62450.2024.00034

Haq Hashmi, A., Mir, G. U., Sattar, K., Ullah, S. S., Alroobaea, R., Iqbal, J., & Hussain, S. (2024). Effects of IoT Communication Protocols for Precision Agriculture in Outdoor Environments. IEEE Access, 12, 46410-46421. https://doi.org/10.1109/ACCESS.2024.3381522

Hassan, M., Ali, E., & Saeed, R. (2024). Intelligent Internet of things in wireless networks. En Intelligent Wireless Communications (págs. 135-162). https://doi.org/10.1049/PBTE094E_ch6

He, Z., Chen, L., Li, F., & Jin, G. (2023). Congestion Avoidance in Intelligent Transport Networks Based on WSN-IoT through Controlling Data Rate

of Zigbee Protocol by Learning Automata. Electronics, 12(9), 1-21. https://doi.org/10.3390/electronics12092070

Hesam Nejati, S. A., Mostafa Razavi, G., Farnoush, N., & Masoud, N. T. (2024). A comprehensive review of energy harvesting and routing strategies for IoT sensors sustainability and communication technology. Sensors International, 5, 100258. https://doi.org/10.1016/j.sintl.2023.100258

Hopjan, M. (2021). Mesh Network Application. 2021 International Conference on Military Technologies-ICMT (págs. 1-4). IEEE. https://doi.org/10.1109/ICMT52455.2021.9502829

Hua, Q., Ni, L., Tao, W., Gelan, Y., & Yang, P. (2024). CDT: Cross-interfData Transfer scheme for bandwidth-efficient LoRa communications in energy harvesting multi-hop wireless networks. Journal of Network and Computer Applications, 229, 103935. https://doi.org/10.1016/j.jnca.2024.103935

Jeknić, A., & Kocan, E. (2023). Development steps that brought to Wi-Fi 7. ETF Journal of Electrical Engineering, 29, 65-79. https://doi.org/10.59497/jee.v29i1.266

Kaur, G., & Chanak, P. (2023). An Intelligent Fault Tolerant Data Routing Scheme for Wireless Sensor Network-Assisted Industrial Internet of Things. IEEE Transactions on Industrial Informatics, 19(4), 5543-5553. https://doi.org/10.1109/TII.2022.3204560

Kim, S. (2023). Hierarchical Multi-Service Resource Allocation Scheme for Future Wireless Network Virtualization. IEEE Access, 11, 87859-87868. https://doi.org/10.1109/ACCESS.2023.3304632

Manali, G., & Khushboo, J. (2024). A Comprehensive Survey of Aerial Mesh Networks (AMN): Characteristics, Application, Open Issues, Challenges, and Research Directions. Wireless Pers Commun(138), 333–368. https://doi.org/https://doi.org/10.1007/s11277-024-11503-7

Marcel Bawindsom, K., Wendpanga Rodrigue, K., Sidi Mohamed, G., Paul, T., & Sawadogo, A. (2024). 2024 IEEE Multi-conference on Natural and Engineering Sciences for Sahel's Sustainable Development (MNE3SD). Enhancing Broadband Access in Urban Burkina Faso: A GIS and Machine Learning-Based Geomarketing Approach to FTTx Potential and Alternatives. IEEE. https://doi.org/10.1109/MNE3SD63831.2024.10812152

Martín-Pascual, M., & Andreu-Sánchez, C. (2023). Practical Application of Mesh Opportunistic Networks. Applied System Innovation, 6(3). https://doi.org/10.3390/asi6030060

Mohan, S., & Panda, S. (2024). 2024 IEEE International Conference of Electron Devices Society Kolkata Chapter (EDKCON). An Integrated Framework for Real-Time Analysis and Observability of Wireless Sensor Data Using

AWS Edge Service Capabilities (págs. 89-94). IEEE. https://doi.org/10.1109/EDKCON62339.2024.10870672

Mok Shao, T., Mau-Luen, T., Yi Jie, W., & Yoong Choon, C. (2024). 2024 IEEE 12th Conference on Systems, Process & Control (ICSPC). Performance Evaluation of Video Streaming in Wireless Mesh Networks, (págs. 390-394). https://doi.org/10.1109/ICSPC63060.2024.10862838

Mozaffariahrar, E., Theoleyre, F., & Menth , M. (2022). A Survey of Wi-Fi 6: Technologies, Advances, and Challenges. Future Internet, 14(10). https://doi.org/10.3390/fi14100293

Murad, S., Badeel, R., Abdal, B., Rahman, T., & Al-Quraishi, T. (2024). Introduction to Wi-Fi 7: A Review of History, Applications, Challenges, Economical Impact and Research Development. Mesopotamian Journal of Computer Science, 2024, 110-121. https://doi.org/10.58496/MJCSC/2024/009

Neema, M., Gopi, E., & Pulakunta Sandeep, R. (2023). Optimizing Broadband Access and Network Design in Wireless Mesh Networks using Multi-Objective Particle Swarm Optimization. Procedia Computer Science, 230, 275-286. https://doi.org/10.1016/j.procs.2023.12.083

Ornelas-Gutierrez, A., Vargas-Rosales, C., & Villalpando-Hernandez, R. (2023). Vehicular Ad Hoc Network Interference Mitigation Using Digital Beamforming Approach in Roundabout Scenarios. IEEE Access, 11, 108232-108244. https://doi.org/10.1109/ACCESS.2023.3321567

Patil, K., & Banerjee, S. (2023). Brief Overview on Wireless Sensor Network Technologies in the Internet of Things (IoT). International Journal of Engineering and Management Research, 13(6), 1-8. https://doi.org/10.31033/ijemr.13.6.1

Piardi, L., Leitao, P., Costa, P., & Schneider de Oliveira, A. (2024). Service Oriented, Holonic and Multi-Agent Manufacturing Systems for Industry of the Future. Collaboration and Self-organization to Enable Self-healing in Industrial Cyber-Physical Systems (págs. 532-543). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-53445-4_44

Qudus, O. A., Ifeanyi, K. E., Bello, A.-R. A., Obafisoye, S., & Ebipade, E. A. (2025). Edge computing and next generation wireless networks: A synergistic approach for efficient sensor data processing. International Journal of Future Engineering Innovations, 2(3), 69-76. https://doi.org/10.54660/IJFEI.2025.2.3.69-76

Reshef, E., Vituri, S., & Gurevitz, A. (2024). Wi-Fi 7 – Technology Realities and Way Forward. 2024 IEEE International Conference on Microwaves, Communications, Antennas, Biomedical Engineering and Electronic Systems-COMCAS (págs. 1-5). IEEE. https://doi.org/10.1109/COMCAS58210.2024.10666165

Rodríguez-Mejía, J. A., Sendra, S., Ivars-Palomares, A., & Lloret, J. (2024). 2024 19th International Symposium on Wireless Communication Systems (ISWCS). Intelligent Heterogeneous Wireless Sensor Networks in Precision Agriculture (págs. 1-6). IEEE. https://doi.org/10.1109/ISWCS61526.2024.10639132

Son, V., & Khoa, N. (2019). Evaluation of Full-Mesh Networks for Smart Home Applications. 2019 International Symposium on Electrical and Electronics Engineering-ISEE, (págs. 73-78). https://doi.org/10.1109/ISEE2.2019.8920920

Sujai, S., Sahoo, G. S., & Awasthi, A. (2024). 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT). Different Mobility Protocol Overview for Wireless Mesh Networks, (págs. 1-6). https://doi.org/10.1109/ICCCNT61001.2024.10725115

Tokhirov, E., & Aliev, R. (2023). Analysis of the differences between Wi-Fi 6 and Wi-Fi 5. E3S Web of Conferences, 402, 1-6. https://doi.org/10.1051/e3sconf/202340203020

Venegas Lorenti, M., Su, Y., Xiang, Y., Nguyen, K., & Sekiya, H. (2024). 2024 15th International Conference on Information and Communication Technology Convergence (ICTC). Combining In-Band SDN and Wireless Mesh Networks for Internet Provisioning in Rural Areas, (págs. 1828-1832). https://doi.org/10.1109/ICTC62082.2024.10827574

Wang, J., Huang, G., & Shao, Z. (2022). Performance Evaluation of Wi-Fi 6 and Technology Prospects of Wi-Fi. 2022 International Conference on Information Processing and Network Provisioning-ICIPNP (págs. 91-95). IEEE. https://doi.org/10.1109/ICIPNP57450.2022.00026

Wang, Z., Kong, L., Shangguan, L., He, L., Xu, K., Cao, Y., . . . Chen, G. (2023). IEEE INFOCOM 2023 - IEEE Conference on Computer Communications. LigBee: Symbol-Level Cross-Technology Communication from LoRa to ZigBee (págs. 1-10). IEEE. https://doi.org/10.1109/INFOCOM53939.2023.10229005

Xinzheng, F., Jun, W., Yulei, W., Jianhua, L., & Wu, Y. (2023). Blockchain and digital twin empowered trustworthy self-healing for edge-AI enabled industrial Internet of things. Information Sciences, 642, 119169. https://doi.org/10.1016/j.ins.2023.119169

Capítulo7: Regulaciones y Normativa

En el ámbito de las telecomunicaciones, las redes inalámbricas desempeñan un papel esencial al facilitar la conexión entre personas y dispositivos, no obstante, su utilización está regulada por un marco normativo complejo, que varía según las jurisdicciones internacionales, regionales y nacionales. Estas regulaciones tienen como objetivo garantizar el uso eficiente y seguro del espectro radioeléctrico, proteger los derechos de los usuarios y promover la sostenibilidad ambiental mediante la implementación de normas técnicas y ambientales específicas. Este capítulo examina las principales legislaciones que rigen el uso de frecuencias a nivel global y local, así como los estándares técnicos y ambientales que deben cumplir las redes inalámbricas, además, se abordan las implicaciones legales asociadas a la seguridad en entornos inalámbricos, destacando cómo estos marcos normativos influyen directamente en el diseño, la implementación y la operación de dichas redes. El análisis ofrecido permitirá al lector comprender de forma integral el impacto de la regulación en el desarrollo y funcionamiento de una infraestructura inalámbrica moderna y responsable.

Objetivos:

- Identificar la legislación internacional relacionada con el uso de frecuencias en redes inalámbricas.
- Analizar las normas específicas aplicables en diferentes regiones.
- Comprender los estándares ambientales y técnicos aplicables a redes inalámbricas.
- Evaluar las implicaciones legales relacionadas con la seguridad en redes inalámbricas.

1.1. Implicaciones Legales de la Seguridad Inalámbrica

El crecimiento acelerado de las redes inalámbricas ha traído consigo desafíos significativos en términos de seguridad y privacidad, y a medida que los ataques cibernéticos se vuelven más sofisticados y la dependencia de las redes inalámbricas crece en sectores críticos como la banca, la salud y las infraestructuras gubernamentales, los gobiernos y organismos reguladores han desarrollado normativas legales estrictas para garantizar la protección de los datos y la privacidad de los usuarios.

El incremento del uso de dispositivos móviles y el auge del Internet de las Cosas (IoT) han multiplicado los riesgos de seguridad, ya que las redes inalámbricas pueden ser vulnerables a ataques como la interceptación de datos, el espionaje electrónico y la suplantación de identidad, como resultado, la legislación en torno a la seguridad inalámbrica no solo ha crecido en cantidad, sino que también ha evolucionado en complejidad para abordar desafíos emergentes en un entorno digital cada vez más interconectado.

Las normativas de seguridad informática no solo regulan la protección de datos personales, sino que también establecen directrices sobre la responsabilidad de los proveedores de servicios, el cumplimiento de estándares internacionales de ciberseguridad, y las medidas para la prevención y gestión de ciberataques. Además, el avance en tecnologías de autenticación y cifrado ha obligado a los gobiernos a actualizar continuamente las regulaciones para asegurar que las redes inalámbricas sean confiables y resistentes a las amenazas cibernéticas.

Por lo tanto, estas implicaciones legales de la seguridad inalámbrica abarcan aspectos como la protección de datos personales, la responsabilidad de los proveedores de servicios, la ciberseguridad en infraestructuras críticas, y la conformidad con estándares internacionales de seguridad. Además, diferentes regiones han establecido leyes específicas para regular el uso y la protección de las redes inalámbricas, buscando equilibrar la innovación tecnológica con la seguridad de los ciudadanos (Hazazi et al., 2018).

1.2. Regulaciones Internacionales sobre Seguridad Inalámbrica

Dado que las redes inalámbricas operan a nivel global, diversas normativas han sido implementadas para estandarizar las prácticas de seguridad y privacidad, protegiendo tanto a empresas como a usuarios, donde dichas regulaciones buscan mitigar riesgos como la interceptación de datos, la manipulación de información y el acceso no autorizado a sistemas críticos, de tal forma que se puede mencionar algunas de las regulaciones más relevantes:

Regulación en la Unión Europea

La Unión Europea ha sido pionera en la regulación de la seguridad y privacidad en las redes inalámbricas, estableciendo estrictos marcos normativos para garantizar la protección de los datos de los ciudadanos:

- **Reglamento General de Protección de Datos (GDPR):** Exige que cualquier entidad que maneje datos personales en redes inalámbricas garantice su seguridad y privacidad, donde se han establecido sanciones de hasta el 4% de la facturación anual de una empresa en caso de incumplimiento.
- **Directiva NIS2:** Refuerza la seguridad de las redes y sistemas de información en la UE, exigiendo medidas estrictas de ciberseguridad para sectores críticos como telecomunicaciones, energía, salud y finanzas.
- **Directiva ePrivacy:** Complementa al GDPR en el ámbito de las comunicaciones electrónicas, regulando el almacenamiento y procesamiento de datos en redes públicas.

Regulación en Estados Unidos

En Estados Unidos, las regulaciones en seguridad inalámbrica se centran en la protección de la privacidad y la prevención del acceso indebido a comunicaciones digitales:

- **Ley de Privacidad de Comunicaciones Electrónicas (ECPA):** Protege la privacidad de las comunicaciones electrónicas y restringe la vigilancia sin orden judicial.
- **Ley de Modernización de la Seguridad Cibernética:** Exige que las empresas informen sobre violaciones de seguridad en entornos digitales y adopten medidas de mitigación.
- **Ley CLOUD Act:** Regula el acceso gubernamental a datos almacenados en servidores de empresas estadounidenses, las mismas que son transmitidas por las redes de datos.

Regulaciones en otras regiones

- **Ley de Protección de Datos de Brasil (LGPD):** Similar a la GDPR, regula la recopilación y el uso de datos los mismos que son transmitidos por los diferentes tipos de redes de datos, estableciendo requisitos para el tratamiento y almacenamiento seguro de la información.

- **Ley de Ciberseguridad de China:** Requiere que las empresas implementen estrictas medidas para el almacenamiento de datos dentro del país, garantizando que las operaciones digitales sean monitoreadas por el gobierno chino.
- **Regulaciones de la ITU (Unión Internacional de Telecomunicaciones)**: Promueven la estandarización global de seguridad en redes de datos, asegurando la interoperabilidad y el uso eficiente del espectro radioeléctrico.

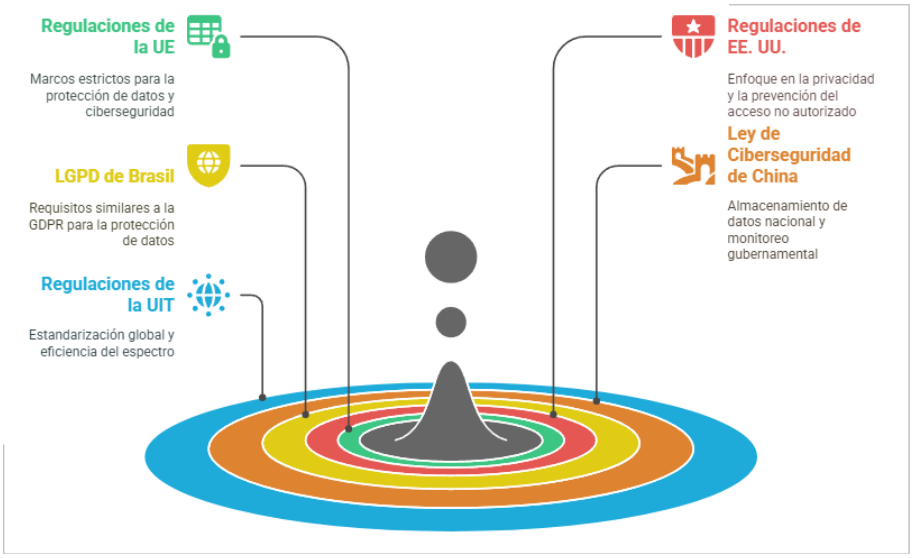

Imagen 33: Regulaciones Internacionales para la Seguridad Inalámbrica.
Fuente: Elaboración propia.

Estas regulaciones establecen el marco legal para la seguridad de las redes inalámbricas y definen las responsabilidades de los proveedores de servicios y empresas tecnológicas, se puede indicar que, en un entorno donde la conectividad inalámbrica sigue expandiéndose, la conformidad con estos marcos regulatorios se ha vuelto indispensable para garantizar la protección de los datos y la integridad de la infraestructura digital (Thakur y Khan Pathan, 2020).

1.3. Desafíos Legales en la Seguridad de Redes Inalámbricas

A pesar de la existencia de normativas, la implementación de medidas de seguridad en redes inalámbricas enfrenta varios desafíos legales y técnicos, donde la naturaleza descentralizada y la facilidad de acceso a estas redes generan riesgos significativos que pueden comprometer la privacidad y la seguridad de la información transmitida, de tal forma que se pueden mencionar los principales desafíos:

Protección de la privacidad y datos personales

Las redes inalámbricas transmiten grandes volúmenes de datos, lo que aumenta el riesgo de exposición de información sensible y la falta de cifrado adecuado y la presencia de redes abiertas facilitan ataques como la intercepción de datos, el espionaje digital, el hacking de redes públicas y la recolección ilegal de metadatos.

Algunas legislaciones, como el GDPR en Europa y la Ley de Privacidad de las Comunicaciones Electrónicas (ECPA) en EE.UU., buscan mitigar estos riesgos imponiendo estrictos requisitos de seguridad para el procesamiento y almacenamiento de datos transmitidos por redes inalámbricas, sin embargo, la implementación de estas normativas sigue siendo desigual en muchas regiones.

Responsabilidad de los proveedores de servicios

Las leyes varían en cuanto a la responsabilidad de los proveedores de servicios de Internet (ISP) y administradores de redes en casos de filtraciones de datos, dando paso a que algunas regulaciones exijan que los ISP tomen medidas activas para prevenir ataques, como la adopción de protocolos de seguridad avanzados y la monitorización de tráfico sospechoso, mientras que otras solo los obligan a reportar incidentes sin intervenir de manera preventiva.

Los desafíos surgen cuando los marcos legales no establecen con claridad hasta qué punto los proveedores de servicios deben ser responsables de la seguridad de los datos en tránsito, y, además, la creciente tendencia de los gobiernos a exigir la retención de datos por parte de los ISP para fines de seguridad nacional genera preocupaciones sobre la privacidad y los derechos digitales de los usuarios.

Ciberseguridad en infraestructuras críticas

Las redes inalámbricas juegan un papel fundamental en infraestructuras críticas como hospitales, sistemas de transporte, telecomunicaciones, redes eléctricas y defensa nacional, donde un ciberataque dirigido a estas infraestructuras podría tener consecuencias devastadoras, incluyendo la interrupción de servicios esenciales y la filtración de información sensible.

Diferentes países han implementado regulaciones para proteger estos sectores, como, por ejemplo, en la Unión Europea, la Directiva NIS2 establece requisitos específicos para la ciberseguridad de infraestructuras críticas, mientras que, en EE.UU., la Ley de Modernización de la Seguridad Cibernética obliga a las empresas que

operan infraestructuras esenciales a notificar cualquier incidente de seguridad y adoptar estrategias de defensa contra ataques cibernéticos.

No obstante, la falta de una estandarización global en la protección de infraestructuras críticas sigue siendo un desafío, lo que deja expuestos a diversos países y sectores ante amenazas cibernéticas transnacionales.

Acceso gubernamental y vigilancia

El equilibrio entre la seguridad y la privacidad ha generado controversias sobre el acceso gubernamental sobre las redes de datos, en algunos países, las leyes permiten la interceptación de datos con órdenes judiciales, mientras que en otros existen restricciones estrictas para proteger la privacidad de los usuarios.

Por ejemplo, la Ley CLOUD Act en EE. UU. facilita el acceso gubernamental a datos almacenados en servidores de empresas estadounidenses, incluso si dichos datos pertenecen a ciudadanos extranjeros, otro ejemplo puede ser en China, donde la Ley de Ciberseguridad obliga a las empresas a cooperar con el gobierno en la vigilancia digital. En contraste, en la Unión Europea, el GDPR y la Directiva ePrivacy imponen estrictas restricciones al monitoreo gubernamental de las comunicaciones privadas.

Estas diferencias en la legislación global han llevado a conflictos diplomáticos y han planteado desafíos en la cooperación internacional en materia de ciberseguridad y privacidad digital (Romero Torres, 2021).

1.4. Responsabilidades de Empresas y Usuarios

El cumplimiento de las regulaciones de seguridad informática no solo recae en los gobiernos, sino también en las empresas y usuarios finales, y para garantizar una protección efectiva de los datos y minimizar las amenazas cibernéticas, es crucial que cada actor asuma su papel en la seguridad como en el caso de las redes inalámbricas.

Empresas y proveedores de servicios

Las empresas de telecomunicaciones, desarrolladores de hardware y proveedores de servicios de Internet deben cumplir con estrictas regulaciones de seguridad para proteger a sus usuarios, entre sus principales responsabilidades se incluyen:

- **Implementación de protocolos de cifrado avanzados:** Se recomienda el uso de WPA3, TLS/SSL y cifrado AES de 256 bits para la protección de datos en tránsito.

- **Cumplimiento con normativas internacionales de ciberseguridad:** Las empresas deben adherirse a estándares como ISO/IEC 27001 (seguridad de la información), NIST Cybersecurity Framework (gestión de riesgos cibernéticos) y SOC 2 (protección de datos en la nube).
- **Seguridad en redes de IoT y 5G:** Con la proliferación de dispositivos IoT y el despliegue de redes 5G, los proveedores deben garantizar la implementación de arquitecturas de seguridad basadas en zero-trust y segmentación de red para reducir la exposición a ataques cibernéticos.
- **Monitoreo y detección de amenazas en tiempo real:** Se requiere el uso de inteligencia artificial y machine learning para detectar comportamientos anómalos en las arquitecturas tecnológicas.
- **Transparencia y notificación de incidentes de seguridad:** En caso de una vulneración, las empresas deben informar a los usuarios y a las autoridades pertinentes en cumplimiento con regulaciones según su región.

Usuarios finales

Los usuarios también desempeñan un papel crucial en la protección de sus datos y dispositivos al conectarse a redes inalámbricas, entre sus principales responsabilidades se encuentran:

- **Evitar el uso de redes Wi-Fi públicas no seguras:** Las redes abiertas son vulnerables a ataques como el man-in-the-middle (MitM), donde los atacantes pueden interceptar datos personales.
- **Configurar contraseñas seguras y autenticación multifactor:** Se recomienda utilizar contraseñas de al menos 12 caracteres, junto con autenticación de doble factor (2FA) o biometría.
- **Uso de VPNs (redes privadas virtuales):** Una VPN cifrada puede proteger la navegación en redes Wi-Fi públicas y prevenir el rastreo de la actividad en línea.
- **Actualizar dispositivos y software regularmente:** Mantener el firmware de routers y sistemas operativos actualizados ayuda a prevenir vulnerabilidades explotadas por cibercriminales.
- **Deshabilitar la conectividad automática a redes Wi-Fi desconocidas:** Esto evita que los dispositivos se conecten inadvertidamente a redes inseguras.

El cumplimiento de estas prácticas reduce significativamente el riesgo de ataques y ayuda a proteger la integridad de las redes inalámbricas, donde la colaboración entre gobiernos, empresas y usuarios es esencial

para construir un entorno digital más seguro y resiliente frente a amenazas emergentes.

1.5. Regulación y Normativas en el Ecuador

La regulación y normativas de las redes de datos en Ecuador han sido desarrolladas con el objetivo de garantizar la seguridad, interoperabilidad y expansión de los servicios de telecomunicaciones en el país, donde la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) es el organismo encargado de administrar el espectro radioeléctrico y supervisar el cumplimiento de la legislación vigente en el sector de las telecomunicaciones.

La normativa ecuatoriana ha evolucionado en los últimos años para abordar desafíos como la expansión de redes en zonas rurales, la ciberseguridad, la asignación del espectro radioeléctrico y el cumplimiento de estándares internacionales.

Ley Orgánica de Telecomunicaciones

La Ley Orgánica de Telecomunicaciones establece el régimen legal para la administración, control y uso del espectro radioeléctrico, y sus principales disposiciones incluyen:

- La administración exclusiva del espectro radioeléctrico por parte del Estado.
- Regulación de la concesión de títulos habilitantes para operadores de telecomunicaciones.
- Sanciones a las infracciones cometidas por operadores sin licencia.
- Promoción de la competencia en el sector de telecomunicaciones.

Por lo tanto, ARCOTEL es la entidad responsable de aplicar esta ley y de sancionar a operadores que incumplan con las regulaciones establecidas.

Regulación del Espectro Radioeléctrico

El espectro radioeléctrico es un recurso estratégico en Ecuador y su uso está sujeto a regulaciones específicas, de tal forma que ARCOTEL establece ciertas normativas:

- Asignación de frecuencias para operadores de telecomunicaciones.
- Uso de bandas de frecuencia para servicios móviles e inalámbricos.
- Requisitos técnicos para la implementación de redes inalámbricas.
- Fiscalización de interferencias y control del uso del espectro.

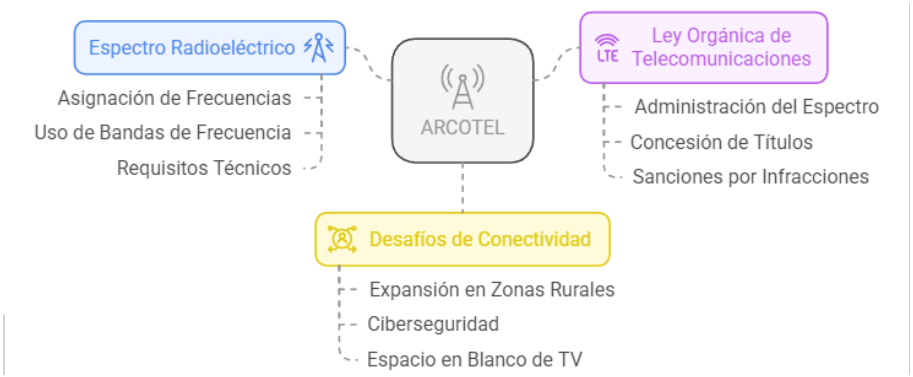

Imagen 34: Regulación de Telecomunicaciones en Ecuador.
Fuente: Elaboración propia.

Además, Ecuador ha explorado el uso del espacio en blanco de TV (TV White Spaces, TVWS) para mejorar la conectividad en zonas rurales y reducir la brecha digital, tal como se muestra a continuación:

- **Modelos de propagación ajustados para zonas rurales montañosas:** Se han desarrollado modelos de propagación específicos para TVWS adaptados a topografía montañosa como la del Ecuador andino, mejorando la precisión del diseño de cobertura para zonas rurales (Caceres Chanaga et al., 2024).
- **Uso de plataformas de evaluación espectral:** Se han desarrollado interfaces gráficas para analizar el espectro de TVWS, las cuales permiten identificar los canales disponibles para dispositivos secundarios, tomando en cuenta la normativa vigente en cada país, lo que posibilitaría a Ecuador examinar regiones específicas de interés.

1.6. Desafíos de la Regulación en Ecuador

A pesar del avance en la normativa de telecomunicaciones, Ecuador enfrenta múltiples desafíos en la regulación de redes inalámbricas, entre los cuales se destacan:

Expansión de Redes en Zonas Rurales

El acceso a servicios de telecomunicaciones en zonas rurales sigue siendo limitado debido a factores como:

- Dificultades geográficas para el despliegue de infraestructura.
- Bajos incentivos económicos para los operadores.
- Necesidad de mayores inversiones en tecnologías como CDMA 450 y TVWS para mejorar la cobertura.

Ciberseguridad

La ciberseguridad en Ecuador enfrenta importantes desafíos regulatorios, especialmente en el contexto de la expansión de redes inalámbricas hacia zonas rurales. Aunque existen esfuerzos para fortalecer la protección de datos y la infraestructura digital, aún se evidencian vacíos legales y operativos:

- **Falta de un marco normativo robusto:** Diversos estudios han señalado que las leyes actuales en Ecuador no son suficientes para prevenir adecuadamente los riesgos cibernéticos ni para implementar estándares internacionales como ISO/IEC 27001 o el marco NIST de forma generalizada. Por ejemplo, un análisis sobre el Ministerio de Educación de Ecuador propuso un marco híbrido basado en ISO 27005 y NIST 800-53 para gestionar los riesgos de ciberseguridad, dado que las infraestructuras tecnológicas presentan vulnerabilidades críticas como accesos no autorizados y contraseñas débiles (De la Torre et al., 2024).
- **Necesidad de certificaciones y modelos efectivos:** Un estudio de caso en el Registro de la Propiedad del Cantón Pedro Moncayo demostró que la implementación de un Sistema de Gestión de Seguridad de la Información (ISMS) bajo ISO/IEC 27001:2013 contribuyó significativamente a proteger los datos públicos, pero también evidenció que este tipo de prácticas aún no están estandarizadas a nivel nacional (Tintin y Hidalgo, 2023).
- **Ciberdefensa estatal limitada frente a nuevas amenazas:** Un análisis desde la perspectiva de defensa nacional indica que, pese a existir políticas de ciberseguridad, el país aún está lejos de garantizar un ciberespacio plenamente seguro, especialmente considerando amenazas emergentes que

podrían afectar redes críticas en zonas aisladas o de difícil acceso (Semanate Esquivel y Recalde, 2023).

Regulación de Operadores Virtuales

La concesión de títulos habilitantes para operadores móviles virtuales (MVNO) es un tema en discusión en Ecuador, y se ha propuesto la creación de un marco regulatorio específico que defina los derechos y deberes de estos operadores, con el fin de fomentar la competencia y mejorar la oferta de servicios móviles.

1.7. Perspectivas Futuras en la Regulación

El marco regulatorio de Ecuador debe continuar evolucionando para adaptarse a los avances tecnológicos y mejorar el acceso a las telecomunicaciones en el país, algunas iniciativas clave incluyen:

Implementación de Redes 5G

Ecuador se encuentra actualmente en fase de evaluación para la asignación del espectro necesario para redes 5G. Las futuras regulaciones deben incluir:

- Licenciamiento específico para operadores de servicios 5G.
- Lineamientos sobre infraestructura, como torres y antenas, compatibles con redes existentes.
- Normativas claras para la protección de datos y la privacidad en ambientes de alta conectividad.

La adopción de 5G se considera clave para reducir la brecha digital, ya que su capacidad para manejar múltiples dispositivos y entornos con alta densidad de usuarios permitiría establecer comunicaciones confiables en tiempo real, incluso en comunidades remotas (Pazmino et al., 2023).

Uso de Inteligencia Artificial

La inteligencia artificial está emergiendo como una herramienta prometedora para mejorar la eficiencia regulatoria. Su aplicación permitiría:

- Monitorear de forma automatizada el uso del espectro radioeléctrico.
- Detectar y mitigar interferencias de manera predictiva.

- Optimizar la planificación de redes inalámbricas, especialmente en áreas rurales donde los recursos técnicos y humanos son más limitados.

Investigaciones recientes en Ecuador indican que la inteligencia artificial puede incorporarse en procesos operativos de distintos sectores para optimizar la toma de decisiones y abordar obstáculos regulatorios, destacando su valor como herramienta para mejorar la gestión tecnológica por parte de las entidades reguladoras.

Expansión de Políticas de Inclusión Digital

El gobierno ecuatoriano ha promovido políticas para cerrar la brecha digital, incluyendo:

- Creación de zonas de acceso gratuito a Internet en comunidades rurales.
- Subsidios a operadores para desplegar infraestructura en regiones con baja conectividad.
- Alianzas con el sector privado para desarrollar proyectos de inclusión digital

1.8. Caso de Estudio

Una empresa de tecnología ubicada en un país de la Unión Europea planea implementar una red inalámbrica de gran alcance, ya que, durante el proceso de diseño, deben considerar las regulaciones sobre potencia y bandas de frecuencia, así como el cumplimiento del GDPR para proteger los datos de los usuarios. Además, se enfrenta al desafío de implementar dispositivos que cumplan con los estándares IEC y ISO para minimizar su huella ambiental, donde el incumplimiento podría resultar en multas significativas y daños a su reputación corporativa.

Preguntas para el análisis:

1. ¿Cómo debería proceder la empresa para cumplir con todas las regulaciones?
2. Si la empresa no cumple con el GDPR, ¿qué tipo de consecuencias técnicas y legales podría enfrentar en la implementación de su red inalámbrica?
3. ¿Cuáles podrían ser las estrategias más efectivas para garantizar que la red inalámbrica cumpla con los requisitos del GDPR sin comprometer la eficiencia operativa de la empresa?

1.9. Resumen Ejecutivo del Capítulo

Este capítulo abordó el marco legal y normativo que rige el uso y la seguridad de las redes inalámbricas, donde se analizan las implicaciones legales de proteger la información transmitida y los riesgos de accesos no autorizados. Se presentan las principales regulaciones internacionales como las emitidas por la ITU, FCC y la Unión Europea, las mismas que garantizan el uso adecuado del espectro radioeléctrico y la interoperabilidad entre dispositivos. Además, se revisan los desafíos legales asociados al crecimiento del IoT y la necesidad de normativas específicas, ya que, en el contexto ecuatoriano, se discute la legislación nacional sobre telecomunicaciones, su alineación con estándares globales y los retos para su implementación efectiva. Se exploraron las perspectivas futuras, incluyendo la necesidad de políticas adaptativas frente a las tecnologías emergentes, y por último se emplea un caso de estudio donde se muestra cómo una entidad pública gestiona la regulación de redes inalámbricas en zonas rurales.

1.10. Evaluación del capítulo

¿Cuál es la principal organización internacional responsable de regular el espectro radioeléctrico?

a) Federal Communications Commission (FCC)
b) Unión Internacional de Telecomunicaciones (ITU)
c) Agencia Europea de Comunicaciones Electrónicas (CEPT)
d) Comisión Electrotécnica Internacional (IEC)

¿Qué normativa europea obliga a las empresas a proteger los datos personales transmitidos en redes inalámbricas?

a) CFAA
b) GDPR
c) WEEE
d) CEPT

¿Qué organismo regula telecomunicaciones en Ecuador?

a) ARCEP
b) ARCOTEL
c) FCC
d) ISO

Según la normativa ecuatoriana, ¿qué requisito es obligatorio para operar redes inalámbricas comerciales?

a) Licencia ambiental
b) Registro en el Ministerio de Salud

c) Autorización de frecuencia por parte de ARCOTEL
d) Certificación IEEE

¿Qué instrumento legal en Ecuador establece principios y medidas de ciberseguridad para proteger la infraestructura crítica, incluidas las redes inalámbricas?

a) Ley Orgánica de Protección de Datos Personales
b) Código de la Niñez y Adolescencia
c) Política Pública de Ciberseguridad del Ecuador
d) Código de Ética Profesional TIC

REFERENCIAS BIBLIOGRÁFICAS

Caceres Chanaga, J., Acevedo Cardenas, E., & Rodriguez-Ferreira, J. (2024). 2024 34th International Telecommunication Networks and Applications Conference (ITNAC). Radio Propagation Model Adjusted to Mountainous Topography for TVWS Coverage Study (págs. 1-7). IEEE. https://doi.org/10.1109/ITNAC62915.2024.10815272

De la Torre, J., Imbaquingo, D., & Llumiquinga, J. (2024). Computational Science and Its Applications -- ICCSA 2024 Workshops. Hybrid Information Security Framework Based on ISO/IEC 27005:2022 and the NIST Framework for the Ministry of Education of Ecuador (TIC) (págs. 71-85). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-65285-1_6

Navarro Cadavid, A., & Barahona Sepulveda, Y. (2023). 2023 IEEE International Humanitarian Technology Conference (IHTC). Wireless DOCSIS: Experience in Colombian Pacific Coast (págs. 1-6). IEEE. https://doi.org/10.1109/IHTC58960.2023.10508839

Pazmino, L., Flores, F., Becerra, F., Cevallos, G., & Rivera, R. (2023). Proceedings of The 2022 International Conference on Digital Transformation and Innovation Technology. Challenges and Opportunities of 5G Deployment in Ecuador. EasyChair. https://doi.org/10.29007/d4tj

Semanate Esquivel, A., & Recalde, L. L. (2023). El Estado y la defensa del ciberespacio. Revista De La Academia Del Guerra Del Ejército Ecuatoriano, 16(1). https://doi.org/10.24133/AGE.VOL16.N01.2023.07

Thakur, K., & Khan Pathan, A.-S. (2020). Cybersecurity Fundamentals A Real-World Perspective (Primera ed.). CRC Press. https://doi.org/10.1201/9781003035626

Tintin, R., & Hidalgo, M. (2023). 2023 Ninth International Conference on eDemocracy & eGovernment (ICEDEG). Could an ISMS Model (ISO/IEC 27001:2013 Standard) Implementation Really Protect Public Data? (págs. 1-5). IEEE. https://doi.org/10.1109/ICEDEG58167.2023.10122109

ISBN: 978-9942-33-994-2

Compás
capacitación e investigación