Redes inalámbricas y equipos de cómputo: configuración e implementación

Breve descripción:

Este componente aborda los elementos para desarrollar la configuración, instalación y administración de redes inalámbricas, junto con la integración y puesta en marcha de equipos de cómputo. El módulo, también incluye la selección y configuración de dispositivos de red, aplicación de protocolos de seguridad y optimización del rendimiento de conexiones inalámbricas, garantizando la conectividad y funcionalidad de sistemas de cómputo.

Noviembre 2024

Tabla de contenido

Introducción

En la actualidad, las redes inalámbricas son una pieza fundamental en la infraestructura de comunicaciones, permitiendo la conectividad sin cables y facilitando el acceso a la información desde cualquier lugar. Con el auge del Internet de las Cosas (IoT) y la proliferación de dispositivos inteligentes, la necesidad de redes inalámbricas robustas y seguras se ha vuelto imprescindible. Este módulo ofrece una visión integral de las tecnologías, dispositivos y técnicas de configuración principales para la implementación y optimización de redes inalámbricas y su interacción con equipos de cómputo.

El contenido abarca desde las tecnologías base, como Wi-Fi y Bluetooth, hasta los dispositivos específicos de IoT que habilitan la conectividad inteligente, tales como sensores, actuadores y microcontroladores. Estos componentes permiten la creación de entornos conectados que se adaptan a múltiples aplicaciones en áreas como la industria, el hogar y la salud. Comprender la función de cada uno y cómo interactúan en una red compleja es fundamental para lograr un funcionamiento eficiente y adaptado a las necesidades de los usuarios.

Otro aspecto central de este módulo es la infraestructura necesaria para el despliegue de redes inalámbricas, incluyendo la planificación de cobertura, la elección de antenas y los métodos de configuración de Access Points. Estas herramientas permiten que las redes mantengan una cobertura adecuada y estable, asegurando que los dispositivos puedan conectarse de manera óptima y sin interrupciones. A través de estos procesos, los administradores de red pueden controlar el rendimiento y ajustarlo según los requisitos del entorno.

Finalmente, este componente profundiza en los aspectos de seguridad y gestión en redes inalámbricas, abordando protocolos como WPA2 y técnicas avanzadas de monitoreo y autenticación. Con la creciente cantidad de dispositivos conectados y el intercambio constante de datos, asegurar la integridad y confidencialidad de las redes se ha convertido en una prioridad. Esta formación proporciona las herramientas necesarias para implementar políticas de seguridad efectivas, proteger el acceso a la red y mantener un rendimiento confiable en entornos inalámbricos de alta demanda.

¡Bienvenido a este viaje relacionado con la configuración e implementación de los equipos de cómputo!

Video 1. Redes inalámbricas y equipos de cómputo

Enlace de reproducción del video

Síntesis del video: Redes inalámbricas y equipos de cómputo
En el componente formativo «Redes inalámbricas y equipos de cómputo: configuración e implementación», se desarrollan habilidades para configurar y administrar redes inalámbricas, así como para integrar equipos de cómputo de manera efectiva. Este componente también aborda la optimización del rendimiento de las redes inalámbricas mediante técnicas avanzadas de configuración y análisis de señal, asegurando conexiones rápidas y estables. Se promueve el uso de herramientas de gestión de redes para monitorear y resolver problemas de conectividad en tiempo real, garantizando un soporte proactivo y eficiente. Este componente desde la selección de tecnologías y dispositivos hasta la implementación de medidas de seguridad para garantizar un rendimiento óptimo y protegido. En un mundo altamente conectado, las tecnologías inalámbricas como Wi-Fi y Bluetooth son fundamentales para facilitar la comunicación y el acceso a datos sin cables. Comprender las características y aplicaciones de estas tecnologías permite diseñar redes adaptadas a diversas necesidades y entornos, desde oficinas hasta instalaciones industriales y domésticas.

El contenido también incluye la planificación de infraestructuras inalámbricas, considerando aspectos como la cobertura, la colocación de Access Points y la gestión de interferencias.

Estos elementos son necesarios para asegurar una conectividad estable y eficiente, especialmente en áreas con alta densidad de dispositivos.

Un enfoque significativo de este componente es la seguridad en redes inalámbricas, que aborda protocolos como WPA2 y prácticas de autenticación robustas para proteger la información y prevenir accesos no autorizados.

Se enfatiza en el monitoreo continuo para detectar amenazas y optimizar el rendimiento de la red.

¡Bienvenido al recorrido por las tecnologías de comunicación inalámbrica y la infraestructura de equipos de cómputo!

1. Tecnologías inalámbricas

Las tecnologías inalámbricas permiten la transmisión de datos sin necesidad de cables, utilizando ondas electromagnéticas para establecer comunicación entre dispositivos. Estas tecnologías facilitan la conectividad en redes locales y en redes de larga distancia y son decisivas en aplicaciones móviles, redes de área local y dispositivos IoT. Además, cada tecnología inalámbrica tiene características específicas en cuanto a velocidad, alcance y capacidad, adaptándose a diferentes entornos y necesidades de comunicación.

Las tecnologías inalámbricas abarcan una variedad de métodos y estándares de comunicación que van desde redes de área personal, como Bluetooth, hasta redes de área amplia, como las redes celulares 3G, 4G y 5G. Estas tecnologías permiten a los dispositivos conectarse y transferir datos sin restricciones físicas, ofreciendo mayor flexibilidad y accesibilidad. La comunicación inalámbrica ha transformado sectores como la movilidad, el internet de las cosas (IoT) y las redes de sensores, permitiendo que múltiples dispositivos trabajen de manera colaborativa y sin interrupciones físicas.

A medida que las tecnologías inalámbricas avanzan, el enfoque en la eficiencia, la seguridad y la velocidad de transferencia de datos se vuelve cada vez más importante. Las redes inalámbricas deben optimizar el uso del espectro electromagnético y adaptarse a entornos complejos, como áreas urbanas con alta densidad de dispositivos. La implementación de tecnologías como 5G, con mayor velocidad y menor latencia, impulsa una conectividad casi en tiempo real, abriendo posibilidades en aplicaciones avanzadas como la conducción autónoma, la telemedicina y las ciudades inteligentes.

1.1. Estándares y protocolos (WiFi, Bluetooth, 3G/4G/5G).

Los estándares y protocolos inalámbricos definen las reglas y tecnologías que permiten la comunicación entre dispositivos sin cables. Cada estándar tiene características específicas que lo hacen adecuado para ciertos usos y entornos.

- **WiFi (IEEE 802.11)**: principal tecnología para redes locales inalámbricas (WLAN), diseñada para ofrecer conexión de alta velocidad en áreas limitadas, como hogares o espacios de trabajo. Los protocolos más utilizados son 802.11n, 802.11ac y 802.11ax, cada uno con mejoras en velocidad y eficiencia.
- **Bluetooth (IEEE 802.15.1)**: enfocado en la comunicación a corta distancia, Bluetooth es ideal para la conectividad entre dispositivos personales, como teléfonos, auriculares y periféricos. Las versiones más recientes, como Bluetooth 5.0, ofrecen mayor velocidad y cobertura.
- **3G, 4G y 5G**: estos estándares de redes celulares permiten la transmisión de datos a largas distancias, adecuadas para la conectividad móvil. Cada generación ha mejorado en velocidad, latencia y capacidad de conectividad. Mientras que 4G permitió el streaming y la transmisión de grandes volúmenes de datos, 5G habilita una conectividad más rápida y estable, favoreciendo aplicaciones en tiempo real y el IoT a gran escala.

Cada uno de estos estándares y protocolos contribuye a satisfacer diferentes necesidades de conectividad, desde redes locales hasta la comunicación a nivel global.

Figura 1. Estándares y protocolos de conectividad inalámbrica

Fuente. OIT, 2024.

1.2. Espectro electromagnético y propagación

El espectro electromagnético es el rango de todas las frecuencias de ondas electromagnéticas, utilizado para transmitir datos en tecnologías inalámbricas. Las diferentes frecuencias permiten que las señales viajen a distintas velocidades, distancias y niveles de penetración. En telecomunicaciones, las bandas de frecuencia más comunes incluyen las frecuencias de 2.4 GHz y 5 GHz, empleadas en redes WiFi, y frecuencias más bajas y altas en redes móviles como 4G y 5G.

La propagación de la señal depende de factores como la frecuencia utilizada y el entorno en el que se transmite. Las ondas de baja frecuencia pueden cubrir distancias mayores y penetrar de mejor manera, mayores obstáculos, como paredes, pero tienden a tener velocidades de transmisión más bajas. Por otro lado, las ondas de alta

frecuencia ofrecen mayor velocidad, pero su alcance y capacidad de penetración son limitados. Los entornos urbanos densos presentan retos de propagación, como interferencias y atenuación, que afectan la calidad de la señal.

La planificación adecuada del uso del espectro y la comprensión de la propagación son fundamentales para optimizar el rendimiento y la cobertura de redes inalámbricas.

1.3. Arquitecturas inalámbricas

Las arquitecturas inalámbricas son los modelos y configuraciones de red que permiten la interconexión de dispositivos sin necesidad de cables físicos. Estas arquitecturas son fundamentales para organizar y gestionar el tráfico de datos en redes inalámbricas, adaptándose a distintos entornos y necesidades de conectividad. Los dos modelos principales en redes inalámbricas son la arquitectura de infraestructura y la arquitectura ad hoc, cada uno con aplicaciones específicas en función de las características de la red y los requisitos de comunicación.

En una red de infraestructura, los dispositivos se conectan a través de un punto de acceso central, como un router o un access point, que regula y controla la transmisión de datos. Este modelo es común en redes empresariales y domésticas, ya que facilita el control y la seguridad de la red, permitiendo que los dispositivos accedan a la conexión de manera ordenada. Asimismo, las redes de infraestructura permiten una mejor gestión del tráfico de datos, la implementación de medidas de seguridad y una mayor estabilidad en las comunicaciones.

Por otro lado, las redes ad hoc no dependen de un punto de acceso central; en este modelo, los dispositivos se conectan directamente entre sí para intercambiar

información. Las redes ad hoc se utilizan generalmente en situaciones temporales o de emergencia, donde no es posible desplegar una infraestructura fija. Estas redes permiten la creación de conexiones rápidas y flexibles, pero pueden presentar limitaciones en términos de alcance y seguridad debido a la falta de un punto de control central. Este tipo de arquitectura es útil en entornos militares, conferencias, o situaciones de desastre donde se necesita comunicación inmediata.

Cada tipo de arquitectura inalámbrica presenta ventajas y desafíos específicos. Las redes de infraestructura son más adecuadas para entornos donde se requiere un control y una administración centralizados, mientras que las redes ad hoc ofrecen flexibilidad y rapidez en el despliegue, aunque con una estructura menos robusta. La elección de una arquitectura inalámbrica adecuada depende de factores como la cantidad de dispositivos, la seguridad necesaria y el alcance de la red.

Las arquitecturas inalámbricas representan todo un avance en los sistemas de intercomunicación de dispositivos, también presentan aspectos de debilidad como lo es la seguridad y la estabilidad de la conexión en cada tipo de red. Las redes de infraestructura, al depender de un punto central de acceso, pueden implementar protocolos de seguridad más avanzados, como el control de acceso y la autenticación de usuarios. Esto las convierte en una opción más segura y estable para entornos que requieren confidencialidad en la transmisión de datos, como oficinas o instituciones.

Por su parte, las redes ad hoc, al carecer de un nodo de control centralizado, presentan desafíos adicionales en términos de seguridad, ya que cada dispositivo actúa como un nodo independiente. Esto las hace más vulnerables a ataques externos y menos estables cuando se incrementa el número de dispositivos conectados o cuando existen interferencias en el entorno.

2. Dispositivos y componentes IoT

El módulo sobre dispositivos y componentes IoT se enfoca en los elementos indispensables que hacen posible el Internet of Things (IoT), donde los dispositivos están interconectados, comparten información y permiten la automatización y el monitoreo inteligente. La implementación de sistemas IoT requiere de componentes específicos, como sensores, actuadores, gateways y microcontroladores, qué juntos habilitan una comunicación fluida y eficaz en la red, y permiten que los sistemas respondan de manera autónoma según las condiciones detectadas.

Los sensores son dispositivos que recopilan información del entorno y la convierten en datos digitales. Por ejemplo, un sensor de temperatura mide el calor del ambiente y envía estos datos a otros sistemas para que realicen ajustes automáticos, como encender un ventilador. Los sensores son primordiales en aplicaciones de monitoreo y control ambiental, en industrias de manufactura y en entornos domésticos. Por su parte, los actuadores son dispositivos que ejecutan acciones físicas en respuesta a las señales que reciben. Por ejemplo, un actuador puede abrir una válvula o mover un mecanismo, convirtiendo las señales de los sensores en acciones específicas.

Los gateways y controladores desempeñan un papel principal en la infraestructura de redes IoT. Los gateways actúan como intermediarios que traducen los protocolos de comunicación y envían datos de los dispositivos al sistema central, ya sea en el cloud o en servidores locales. Su función es determinante para filtrar, procesar y gestionar el tráfico de datos en tiempo real, garantizando que la información se envíe de manera segura y eficiente. Los controladores, por otro lado, coordinan la

comunicación entre sensores y actuadores, gestionando el flujo de datos y asegurando que las respuestas sean adecuadas y rápidas.

Los microcontroladores y plataformas de procesamiento local o en el cloud permiten que los sistemas IoT analicen datos y tomen decisiones autónomas en función de los algoritmos de programación. Estos dispositivos, como las placas Arduino y Raspberry Pi, son plataformas versátiles que soportan múltiples tipos de sensores y actuadores, facilitando la creación de soluciones personalizadas para aplicaciones específicas. La incorporación de estos microcontroladores permite el procesamiento local, que es particularmente útil en aplicaciones que requieren respuestas inmediatas, mientras que el cloud permite el análisis de grandes volúmenes de datos en un entorno centralizado.

Cada uno de estos componentes trabaja en conjunto para crear un sistema de comunicación y respuesta que caracteriza a la tecnología IoT. A medida que se desarrollan nuevas aplicaciones en campos como la agricultura, la salud y las ciudades inteligentes, la comprensión profunda de estos dispositivos y componentes se vuelve indispensable para crear redes eficientes y seguras.

Tabla 1. Componentes y funcionalidades clave

Componente	Descripción	Función en la Red
Dispositivos de red.	Equipos como Access Points, routers y controladores.	Facilitan la conectividad y controlan el tráfico de la red.
Sensores IoT.	Dispositivos que capturan datos ambientales (temperatura, movimiento, etc).	Recogen datos y permiten el monitoreo en tiempo real.

Componente	Descripción	Función en la Red
Protocolos de Seguridad.	Ej. WPA, WPA2, autenticación multifactor (MFA).	Protegen el acceso y garantizan la confidencialidad de la red.
Antenas y coberturas.	Estructuras que amplían o dirigen la señal inalámbrica.	Aseguran una señal estable en toda el área de cobertura.
Monitoreo y Gestión.	Herramientas y métodos de supervisión del tráfico y el rendimiento de la red.	Previenen intrusiones y optimizan el rendimiento de la red.

Fuente. OIT, 2024.

2.1. Sensores y actuadores

Los sensores y actuadores son componentes fundamentales en los sistemas IoT, permitiendo la interacción directa con el entorno y el control de diversos procesos. Los sensores recopilan datos específicos del ambiente, como temperatura, humedad, presión, o niveles de luz, y los convierten en señales digitales que pueden ser interpretadas por otros dispositivos. Este proceso de recolección de datos es primordial para la toma de decisiones automatizadas en sistemas IoT, ya que proporciona la información necesaria para el monitoreo continuo y en tiempo real de condiciones variables en el entorno.

Los actuadores, por otro lado, son dispositivos que convierten las señales digitales en acciones físicas. Por ejemplo, un actuador puede encender una lámpara, abrir una válvula de agua o ajustar el nivel de un termostato. Esta capacidad de respuesta permite que los sistemas IoT no solo recopilen datos, sino que también interactúen activamente con el entorno para realizar tareas específicas en función de los datos que los sensores han proporcionado.

La combinación de sensores y actuadores en un sistema IoT es lo que permite la creación de entornos autónomos y adaptativos. En aplicaciones industriales, esta sinergia facilita la supervisión de maquinaria y la automatización de tareas, mientras que en el hogar puede usarse para sistemas de seguridad, termostatos inteligentes, o iluminación automatizada. En resumen, los sensores detectan cambios y los actuadores responden, formando un ciclo continuo que hace posible la funcionalidad inteligente en estos sistemas.

2.2. Gateways y controladores

Los gateways y controladores desempeñan roles decisivos en la infraestructura de los sistemas IoT, actuando como intermediarios y gestores en la comunicación entre dispositivos y redes. Los gateways son responsables de conectar los dispositivos IoT a la red principal, ya sea a través de redes locales o mediante conexión a la cloud. Estos dispositivos filtran y traducen los datos recibidos de los sensores, asegurando que la información se envíe de forma segura y eficiente a los sistemas de procesamiento central. Los gateways también permiten la interoperabilidad entre dispositivos que utilizan diferentes protocolos de comunicación, facilitando la transmisión de datos en redes complejas y distribuidas.

Los controladores se encargan de gestionar y coordinar las interacciones entre dispositivos dentro de un sistema IoT, actuando como el “cerebro” local que toma decisiones sobre la base de los datos obtenidos de los sensores. En muchos sistemas, los controladores están programados para responder de forma autónoma, enviando instrucciones a los actuadores sin necesidad de intervención humana. Estos dispositivos permiten una comunicación fluida y rápida, especialmente en aplicaciones donde la velocidad de respuesta es crítica, como en sistemas industriales o de seguridad.

En conjunto, los gateways y controladores aseguran la estabilidad y eficiencia de los sistemas IoT. Los gateways manejan la conexión y el flujo de datos, mientras que los controladores procesan la información y gestionan las acciones dentro del sistema, facilitando la autonomía y el control centralizado. Esta organización es especialmente útil en aplicaciones de ciudades inteligentes, agricultura de precisión y automatización del hogar, donde se requiere monitoreo constante y respuesta inmediata.

2.3. Microcontroladores y plataformas

Los microcontroladores y las plataformas de desarrollo son componentes fundamentales en los sistemas IoT, ya que permiten el procesamiento local de datos y la ejecución de instrucciones directamente en los dispositivos. Los microcontroladores, como los presentes en las placas Arduino o ESP8266, son pequeños circuitos integrados que combinan un procesador, memoria y entradas/salidas en un solo chip. Esto les permite realizar cálculos, tomar decisiones y controlar otros componentes, como sensores y actuadores, de manera autónoma y en tiempo real, sin necesidad de conectarse continuamente a un sistema externo.

Las plataformas de desarrollo como Raspberry Pi o Arduino proporcionan entornos de hardware y software que facilitan la creación y prueba de soluciones IoT. Estas plataformas son versátiles y compatibles con una amplia variedad de sensores y actuadores, permitiendo a los desarrolladores diseñar soluciones específicas para aplicaciones en áreas como la automatización del hogar, la agricultura de precisión o la industria 4.0. Regularmente, muchas plataformas son de código abierto, lo que fomenta la innovación y permite que los sistemas se adapten a necesidades particulares.

En el contexto de IoT, los microcontroladores y plataformas de desarrollo permiten un procesamiento de datos más eficiente y rápido, lo que es vital para

aplicaciones que requieren respuestas inmediatas. En sistemas complejos, los microcontroladores pueden actuar como dispositivos de borde (edge devices), procesando los datos localmente y enviando solo información relevante a la cloud para un análisis más profundo. Esto reduce la latencia y permite que los sistemas respondan en tiempo real a los cambios en el entorno.

Además de su rol en el procesamiento local de datos, los microcontroladores y plataformas de desarrollo también destacan por su capacidad de conectividad y su adaptabilidad a diferentes protocolos de comunicación, como WiFi, Bluetooth, LoRa y Zigbee. Esto les permite integrarse en redes más amplias y conectarse con otros dispositivos de manera flexible, facilitando el diseño de soluciones escalables en las que varios dispositivos puedan comunicarse entre sí sin necesidad de intervención humana. Las plataformas también soportan bibliotecas y entornos de programación amigables, como C++, Python o JavaScript, lo que permite una implementación rápida y flexible de aplicaciones, optimizando el desarrollo de prototipos y la integración en infraestructuras IoT complejas.

3. Infraestructura inalámbrica

La infraestructura inalámbrica es la base sobre la cual se establecen las conexiones de red sin cables en entornos que van desde el hogar hasta grandes complejos empresariales y públicos. Este módulo abarca los elementos necesarios para crear una red inalámbrica estable y eficaz, garantizando la conectividad de múltiples dispositivos en tiempo real y sin interrupciones. A través de una adecuada infraestructura inalámbrica, las empresas y organizaciones pueden implementar redes capaces de soportar grandes volúmenes de datos y proporcionar una experiencia de conexión confiable en áreas extensas o con condiciones ambientales desafiantes.

Los Access Points (APs) y controladores son componentes indispensables en cualquier infraestructura inalámbrica. Los APs actúan como enlaces que conectan los dispositivos de la red (como teléfonos, laptops y sensores IoT) al sistema principal y, en última instancia, a Internet. Estos puntos de acceso aseguran que los dispositivos puedan moverse dentro de una cobertura amplia sin perder conexión, lo cual es especialmente útil en oficinas abiertas, almacenes y zonas industriales. Los controladores de red, por su parte, permiten gestionar múltiples APs de manera centralizada, facilitando la configuración, monitoreo y administración de la red y optimizando la experiencia del usuario, incluso en redes con alta demanda de tráfico.

Las antenas son otro pilar fundamental en la infraestructura inalámbrica, ya que determinan la calidad y el alcance de la señal. La elección de la antena adecuada —omnidireccional o direccional— depende del entorno y los objetivos de cobertura. Las antenas omnidireccionales, que emiten señales en todas direcciones, son ideales para cubrir áreas circulares o pequeñas, mientras que las antenas direccionales enfocan la señal hacia una zona específica, maximizando el alcance en esa dirección. La correcta

instalación y orientación de las antenas es fundamental para evitar zonas muertas (dead zones) y lograr una cobertura uniforme.

Para diseñar redes inalámbricas eficientes, es necesario realizar estudios de cobertura conocidos como site surveys, que permiten identificar los mejores puntos para colocar los APs y las antenas. Estas evaluaciones consideran factores físicos del entorno, como paredes, techos, materiales de construcción y posibles interferencias. Realizar un site survey permite prever problemas y asegurarse de que la red ofrecerá la máxima cobertura posible, minimizando las áreas sin señal y evitando interferencias que puedan afectar el rendimiento de la red.

Adicionalmente a la cobertura, la gestión de interferencias es un aspecto primordial de la infraestructura inalámbrica. Las redes inalámbricas pueden verse afectadas por otros dispositivos electrónicos, especialmente en lugares donde existen múltiples redes que operan en frecuencias similares. A través de una planificación adecuada y el uso de canales no superpuestos, los administradores de red pueden minimizar la interferencia y optimizar el rendimiento de la red. La selección de frecuencias y el ajuste de la potencia de transmisión también son aspectos fundamentales que se deben ajustar para evitar solapamientos y mantener una conexión estable.

Finalmente, la seguridad es un componente imprescindible en la infraestructura inalámbrica. Los Access Points y controladores permiten implementar protocolos de seguridad que limitan el acceso y protegen los datos que se transmiten a través de la red. Con configuraciones de autenticación y cifrado avanzado, como WPA3, las redes inalámbricas pueden protegerse contra accesos no autorizados y ataques de intrusión, lo que es altamente relevante para preservar la confidencialidad y la integridad de la

información. La seguridad debe planificarse desde el diseño inicial de la red para asegurar que esta no solo sea eficiente, sino también segura frente a amenazas externas.

Tabla 2. Procedimientos y herramientas de implementación

Etapa del Procedimiento	Descripción	Herramientas Recomendadas
Configuración Inicial	Establecer los parámetros de conexión de red y autenticación.	Router, Access Points, software de configuración.
Análisis de Cobertura	Realizar un estudio de sitio para determinar la distribución de la señal.	Site survey tools, mapas de cobertura, herramientas de monitoreo.
Seguridad y Autenticación	Configurar protocolos de seguridad y autenticación de usuarios.	Servidor RADIUS, autenticación WPA2, sistemas de MFA.
Optimización de Rendimiento	Ajustar ancho de banda y priorización de tráfico para estabilidad.	Software de gestión de tráfico, QoS (Quality of Service).
Monitoreo y Mantenimiento	Supervisar el estado de la red y realizar ajustes según sea necesario.	Herramientas de monitoreo de red, logs de eventos, IDS/IPS.

Fuente. OIT, 2024.

3.1. Access Points y controladores

- **Los Access Points (APs)**

  Son dispositivos fundamentales en la configuración de redes inalámbricas, ya que permiten a los dispositivos conectarse a una red sin necesidad de cables. Su función principal es actuar como intermediarios entre los dispositivos de usuario, como laptops, teléfonos y otros equipos IoT, y la red central, garantizando que estos dispositivos puedan acceder a Internet o a una intranet de manera rápida y estable. Los APs son especialmente importantes en espacios donde una conexión por cable sería impracticable o costosa, como en oficinas grandes, centros de datos y edificios con gran cantidad de usuarios móviles.

  Un aspecto determinante de los Access Points es su capacidad para gestionar la conectividad de múltiples dispositivos simultáneamente. A medida que los dispositivos se mueven por un espacio, los APs garantizan que la señal se mantenga estable y se realice una transición sin interrupciones entre distintos puntos de acceso en la red. Esto es primordial en entornos de alta densidad de usuarios, como campus universitarios o centros comerciales, donde la demanda de conectividad es alta y debe mantenerse la calidad de la conexión en toda el área de cobertura.

- **Los controladores de red**

  Desempeñan un papel complementario e indispensable en la gestión de los Access Points, especialmente en redes grandes. Estos controladores permiten la administración centralizada de varios APs, facilitando la configuración, el monitoreo y el control de la red desde una única interfaz.

Los controladores pueden ajustarse para equilibrar la carga de usuarios entre los APs, redirigiendo la conexión de los dispositivos a aquellos puntos de acceso con menor demanda. Esto optimiza el uso de la red y mejora la experiencia de conexión al evitar la saturación en un único AP.

Asimismo, los controladores ofrecen la ventaja de implementar actualizaciones de seguridad y configuraciones de red de manera automática y uniforme en todos los APs conectados. Esto asegura que toda la infraestructura se mantenga protegida contra vulnerabilidades sin necesidad de actualizaciones individuales en cada punto de acceso. La automatización en el despliegue de configuraciones también facilita la administración en redes complejas, reduciendo los errores y simplificando la labor del equipo de soporte técnico.

Una característica avanzada de los controladores es su capacidad para realizar análisis de tráfico y supervisar el rendimiento de la red. Esto permite identificar y resolver problemas en tiempo real, ya sea optimizando la señal, ajustando el rango de cobertura de los APs, o detectando posibles interferencias. La capacidad de monitoreo también ayuda a prevenir ataques de seguridad mediante la detección de comportamientos anómalos en la red, permitiendo respuestas proactivas que protegen la estabilidad de la red inalámbrica.

3.2. Antenas y cobertura

Las antenas son componentes vitales en las redes inalámbricas, ya que determinan tanto el alcance como la calidad de la señal en un área específica. Estas permiten que la señal inalámbrica se distribuya de forma efectiva, maximizando la

cobertura y minimizando las áreas sin conexión, conocidas como zonas muertas (dead zones). Las antenas se seleccionan y configuran según las características del espacio físico y las necesidades de conectividad, considerando factores como la densidad de usuarios, la ubicación de los dispositivos y los obstáculos que puedan interferir con la señal.

Existen varios tipos de antenas utilizadas en redes inalámbricas, cada una con características específicas. Las antenas omnidireccionales emiten la señal en todas direcciones, lo que las hace ideales para cubrir áreas amplias donde los dispositivos se mueven libremente, como oficinas abiertas o áreas públicas. En cambio, las antenas direccionales enfocan la señal en una dirección específica, proporcionando un alcance más largo y concentrado. Estas son útiles para áreas con rutas establecidas o para conectar edificios cercanos, ya que permiten un control más preciso sobre la dirección de la señal.

Además de la dirección de la señal, las antenas tienen diferentes capacidades de ganancia, medida en decibelios (dBi), que indica la intensidad de la señal emitida. Una antena con mayor ganancia puede cubrir distancias más largas, pero también emite una señal más estrecha, lo que puede ser beneficioso o limitante dependiendo del entorno. La elección de la ganancia adecuada es básica para asegurar una cobertura equilibrada, de modo que la señal llegue a todos los dispositivos sin crear áreas de interferencia ni sobrecargar la red.

Para maximizar la cobertura, la colocación estratégica de las antenas es fundamental. Mediante estudios de cobertura y pruebas en el sitio, conocidos como site surveys, los técnicos pueden determinar los puntos ideales para instalar las antenas, evitando obstáculos y áreas de interferencia. Estos estudios ayudan a asegurar

que la señal sea lo suficientemente fuerte en toda el área deseada y que los dispositivos tengan una conexión estable. La planificación de la cobertura es un paso indispensable en la creación de una red inalámbrica eficiente y confiable.

Otro aspecto relevante es el ajuste de la potencia de transmisión, que permite adaptar la intensidad de la señal según las necesidades del espacio. En áreas donde la densidad de dispositivos es alta, como auditorios o centros de convenciones, ajustar la potencia puede ayudar a reducir la interferencia entre puntos de acceso. Al reducir la potencia en ciertas zonas y aumentarla en otras, es posible optimizar la señal y mejorar la experiencia del usuario sin sacrificar la estabilidad de la red.

3.3. Site surveys y planificación

La planificación de la red inalámbrica mediante estudios de sitio, conocidos como site surveys, es un paso primordial para asegurar una cobertura óptima y confiable en cualquier entorno. Un site survey es una evaluación detallada del área en la que se implementará la red inalámbrica, donde se identifican los obstáculos físicos y las condiciones que pueden afectar la señal, como paredes, techos, materiales de construcción y posibles fuentes de interferencia. Este análisis permite desarrollar una estrategia efectiva para la disposición de los Access Points y antenas, asegurando una conectividad fluida y evitando zonas muertas.

- **Existen varios tipos de site surveys**, cada uno con un enfoque específico. Los site surveys pasivos permiten analizar el entorno sin necesidad de encender los dispositivos de la red, evaluando la distribución de señales externas y la posible interferencia que estas pueden causar. Este tipo de estudio es útil para identificar posibles problemas de interferencia y planificar la ubicación de los APs. Por otro lado, los site surveys activos

implican el despliegue temporal de los dispositivos de la red para evaluar su rendimiento en tiempo real, midiendo la intensidad de la señal y la cobertura en diversas ubicaciones. Esta práctica permite ajustar la configuración y ubicación de los dispositivos antes de la instalación final.

- **La planificación de cobertura** es uno de los objetivos primordiales en un site survey. Este proceso implica calcular la cantidad de Access Points necesarios y su colocación óptima para cubrir todas las áreas de manera uniforme. También se debe considerar la densidad de usuarios en cada zona, puesto que, en áreas de alta demanda, como salas de conferencias, aulas o centros de convenciones, puede ser necesario añadir APs adicionales para manejar el tráfico sin perder rendimiento. La planificación de cobertura asegura que la red sea eficiente y que los usuarios tengan una experiencia estable sin interrupciones, independientemente de su ubicación.

Además de la cobertura, el site survey también permite optimizar la selección de canales y frecuencias para reducir la interferencia entre Access Points y mejorar la eficiencia de la red. En redes de gran escala, es común que varios APs utilicen la misma frecuencia, lo cual puede generar interferencia y reducir la calidad de la señal. A través de un análisis de canales, se puede asignar frecuencias específicas a cada AP, minimizando el solapamiento de señal y asegurando que los dispositivos reciban una señal limpia y consistente.

Otro aspecto importante en la planificación es la identificación de fuentes de interferencia dentro del área. Elementos como paredes de metal, hornos microondas o dispositivos Bluetooth pueden causar interferencia en la señal inalámbrica. Un site

survey detallado permite detectar estas fuentes y realizar ajustes en la configuración de los APs, como cambiar la frecuencia de operación o ajustar la potencia de transmisión, para mitigar el impacto de la interferencia y mantener la calidad de la señal en toda el área.

4. Seguridad en redes inalámbricas

La seguridad en redes inalámbricas es un aspecto fundamental en la implementación de una red confiable, ya que las conexiones inalámbricas son particularmente vulnerables a diversas amenazas de seguridad. Debido a la naturaleza de la transmisión inalámbrica, las señales pueden ser interceptadas o manipuladas si no se toman medidas de seguridad adecuadas. Por ello, es importante emplear prácticas y protocolos que garanticen la confidencialidad, integridad y disponibilidad de los datos que se transmiten a través de la red, protegiendo tanto la información sensible como la infraestructura de la red.

Uno de los métodos más utilizados para proteger redes inalámbricas es la implementación de protocolos de seguridad, como WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) y WPA2. Estos protocolos encriptan la información que circula en la red, dificultando el acceso a los datos transmitidos por personas no autorizadas. Sin embargo, cada protocolo tiene un nivel de seguridad diferente; WEP, por ejemplo, es una tecnología más antigua y vulnerable, mientras que WPA2 es más avanzada y segura. Es importante que las redes actuales implementen, como mínimo, WPA2 para minimizar los riesgos de interceptación y ataques.

La autenticación y el control de acceso son otro pilar de la seguridad en redes inalámbricas. Estos mecanismos aseguran que solo los usuarios y dispositivos autorizados puedan conectarse a la red. Las técnicas de autenticación incluyen contraseñas seguras, autenticación multifactorial (MFA) y certificados digitales. Igualmente, los sistemas de control de acceso pueden dividir la red en diferentes niveles, creando redes de invitados separadas de las redes de uso interno, lo cual minimiza la exposición de la red interna a usuarios no autorizados.

Otro aspecto relevante es el monitoreo y la gestión de la seguridad en tiempo real. A través de herramientas de gestión de redes, es posible detectar y reaccionar ante amenazas o comportamientos anómalos en la red. El monitoreo continuo permite a los administradores de red identificar intentos de acceso no autorizado, detectar puntos de acceso no autorizados o "falsos APs" que imitan la red legítima, y bloquear dispositivos potencialmente peligrosos. La gestión y el monitoreo proactivos son determinantes para mantener la integridad de la red y garantizar una experiencia segura para los usuarios.

Por otra parte, la educación de los usuarios en prácticas seguras también contribuye a la seguridad de las redes inalámbricas. Los usuarios deben ser conscientes de los riesgos potenciales y tomar medidas preventivas, como no conectarse a redes públicas desconocidas, evitar compartir contraseñas y mantener sus dispositivos actualizados. La concienciación sobre los riesgos asociados con la conexión inalámbrica puede ayudar a reducir incidentes de seguridad y mejorar la protección de la red.

4.1. Protocolos de seguridad (WEP, WPA, WPA2)

Los protocolos de seguridad en redes inalámbricas son fundamentales para proteger la información que se transmite y garantizar que solo usuarios autorizados accedan a la red. Los tres protocolos principales —WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) y WPA2— fueron desarrollados para mejorar la seguridad de las redes inalámbricas, especialmente en entornos públicos y corporativos donde las amenazas son mayores. Estos protocolos encriptan la información y autentican los dispositivos que intentan conectarse, dificultando la interceptación y manipulación de datos por personas no autorizadas.

WEP fue uno de los primeros protocolos implementados en redes Wi-Fi, diseñado para proporcionar un nivel básico de seguridad. Este protocolo emplea una clave de encriptación estática, que debía configurarse manualmente en cada dispositivo. Sin embargo, WEP mostró ser vulnerable a ataques debido a su encriptación débil y la reutilización de claves, lo que permite que los atacantes intercepten el tráfico y accedan a la red. Hoy en día, WEP es considerado obsoleto, pero su estudio es importante para comprender la evolución de los protocolos de seguridad en redes inalámbricas.

Para abordar las vulnerabilidades de WEP, se introdujo WPA como un estándar de seguridad mejorado. WPA utiliza el protocolo de integridad de clave temporal (TKIP), que genera una clave de encriptación nueva para cada paquete de datos. Este método mejora la seguridad, ya que no reutiliza las mismas claves y ofrece una protección más dinámica. Aunque WPA es más seguro que WEP, sigue teniendo ciertas vulnerabilidades que lo hacen susceptible a ataques avanzados. Por esta razón, WPA fue una solución temporal mientras se desarrollaba una alternativa más robusta: WPA2.

WPA2 es actualmente el estándar de seguridad recomendado para redes Wi-Fi. Este protocolo introduce el cifrado AES (Advanced Encryption Standard), un método de encriptación mucho más seguro que el utilizado en WEP o WPA. AES utiliza claves de cifrado de 128 o 256 bits, haciendo que la información sea extremadamente difícil de descifrar sin la clave de acceso. Extra a a AES, WPA2 también implementa el protocolo de autenticación CCMP, que garantiza la integridad de los datos y protege contra ataques de red comunes, como el "ataque de repetición".

Para configuraciones de seguridad más avanzadas, especialmente en redes corporativas, es común utilizar WPA2-Enterprise, una variante de WPA2 que permite

autenticación en servidores RADIUS, en lugar de usar una clave compartida. Este método mejora la seguridad, ya que cada usuario tiene credenciales únicas y la red puede monitorear y gestionar cada conexión de forma individual. WPA2-Enterprise es ideal en entornos donde se necesita un control estricto sobre el acceso a la red, ya que proporciona autenticación y control de acceso a nivel de usuario.

Tabla 3. Protocolos de seguridad (WEP, WPA, WPA2, WPA3)

Protocolo de seguridad	Propósito	Consideraciones clave	Ejemplos de aplicación
WEP	Proteger redes inalámbricas mediante cifrado básico de datos.	Vulnerable a ataques; utiliza cifrado estático que se puede descifrar fácilmente.	Redes antiguas que aún emplean WEP por compatibilidad, aunque es poco seguro.
WPA	Mejorar la seguridad frente a WEP con cifrado más robusto y autenticación.	Mayor seguridad que WEP, pero aún con vulnerabilidades; reemplazado progresivamente por WPA2.	Conexiones domésticas y pequeñas empresas que requieren una protección moderada.
WPA2	Proveer alta seguridad para redes inalámbricas con cifrado avanzado.	Implementación de AES para mayor seguridad; requiere hardware compatible.	Redes empresariales y domésticas modernas, estándar en la mayoría de dispositivos actuales.
WPA3	Ofrecer la máxima seguridad en redes modernas con protección avanzada de datos.	Incluye cifrado individualizado para conexiones; ideal para redes que manejan información sensible.	Redes de organizaciones con altos requisitos de seguridad, redes de última generación.

Fuente. OIT, 2024.

4.2. Autenticación y control de acceso

La autenticación y control de acceso en redes inalámbricas son componentes fundamentales para asegurar que solo los dispositivos y usuarios autorizados puedan conectarse a la red. Estos mecanismos no solo protegen la red contra accesos no autorizados, sino que también aseguran que cada usuario esté debidamente identificado y autenticado. La autenticación y control de acceso son fundamentales para evitar intrusiones y mejorar la protección de la información y de los recursos de la red.

Uno de los métodos de autenticación más comunes es el uso de contraseñas seguras o claves de acceso. Este tipo de autenticación es adecuado para redes de uso doméstico o pequeñas empresas, donde cada usuario debe conocer la clave para conectarse. Sin embargo, este método tiene limitaciones en entornos de mayor envergadura, ya que, cuando la clave se comparte con personas no autorizadas, la seguridad de la red se ve comprometida. Asimismo, es difícil gestionar el acceso cuando hay muchos usuarios, ya que todos comparten la misma contraseña.

Para redes empresariales, se suele implementar la autenticación basada en RADIUS (Remote Authentication Dial-In User Service), que utiliza un servidor de autenticación centralizado para gestionar el acceso de los usuarios. Este método permite que cada usuario tenga credenciales únicas, mejorando así el control sobre quién puede acceder a la red. El servidor RADIUS verifica las credenciales de cada usuario y, si son correctas, permite el acceso. Este tipo de autenticación es común en entornos empresariales y en redes públicas, donde se necesita un mayor control sobre el acceso y se requiere registrar el ingreso de cada usuario.

Extra a la autenticación, el control de acceso permite dividir la red en diferentes niveles, separando, por ejemplo, las redes de invitados de las redes internas. Esto es posible mediante el uso de redes virtuales o VLANs (Virtual Local Area Networks), que permiten segmentar el tráfico y limitar el acceso a ciertas áreas de la red. Esta práctica es altamente relevante para minimizar el riesgo de que dispositivos no autorizados accedan a información confidencial o recursos críticos de la red. Adicionalmente, al segmentar la red, se facilita la gestión y el monitoreo del tráfico de datos.

En algunos casos, se utiliza la autenticación multifactor (MFA) como medida adicional de seguridad. La MFA requiere que el usuario proporcione más de una forma de verificación para acceder a la red, como una contraseña junto con un código de verificación temporal o una autenticación biométrica. Este enfoque aumenta significativamente la seguridad, ya que complica el acceso para usuarios no autorizados y reduce el riesgo de que alguien pueda obtener acceso únicamente mediante una contraseña robada o interceptada.

Finalmente, es importante implementar políticas de seguridad y capacitación para que los usuarios comprendan la importancia de la autenticación y el control de acceso. Los administradores de red deben asegurar que los usuarios no compartan sus credenciales y que actualicen sus contraseñas regularmente. La educación y concienciación sobre estas prácticas de seguridad fortalecen la protección de la red y ayudan a mantener un entorno de red seguro y confiable.

4.3. Monitoreo y gestión

El monitoreo y gestión de redes inalámbricas son actividades críticas para garantizar su rendimiento y seguridad. En un entorno inalámbrico, donde los dispositivos se conectan y desconectan constantemente, el monitoreo permite

identificar problemas de rendimiento, posibles intrusiones y amenazas, y también asegura el uso eficiente de los recursos de la red. Mediante herramientas avanzadas de monitoreo, los administradores de red pueden supervisar el tráfico en tiempo real, obtener estadísticas de uso y recibir alertas sobre cualquier actividad sospechosa o anomalía.

Una de las principales funciones del monitoreo es detectar y prevenir intrusiones. Esto es posible gracias a sistemas de detección de intrusos (IDS, Intrusion Detection System) y de prevención de intrusiones (IPS, Intrusion Prevention System), que son capaces de identificar comportamientos sospechosos en la red y responder automáticamente para mitigar las amenazas. Estos sistemas alertan al administrador cuando un dispositivo no autorizado intenta acceder a la red, lo que permite bloquear el acceso o limitar las acciones del dispositivo hasta que se investigue el incidente.

Extra al monitoreo, la gestión de rendimiento es necesaria para mantener la calidad de la conexión y minimizar las interrupciones. La gestión incluye la optimización del ancho de banda y el control de acceso a la red para evitar la congestión en áreas de alta densidad de usuarios. A través de la configuración y ajuste de los Access Points y del análisis del tráfico de red, los administradores pueden asegurar que el ancho de banda se distribuya de forma eficiente y que cada usuario reciba una conexión estable. También es posible priorizar el tráfico de aplicaciones críticas, garantizando que no se vean afectadas por el uso de otros servicios.

El uso de herramientas de análisis de datos en redes inalámbricas ha permitido una evolución significativa en el monitoreo de redes. Estas herramientas generan informes detallados sobre el comportamiento de los dispositivos conectados, las horas de mayor uso y el tipo de tráfico que circula en la red. Esta información permite a los

administradores identificar patrones de uso y anticipar problemas antes de que afecten a los usuarios. Por su parte, los análisis de datos pueden utilizarse para mejorar la seguridad, identificando comportamientos anómalos que podrían indicar intentos de ataque o el uso indebido de la red.

La actualización constante de software y firmware de los dispositivos de red es otra práctica fundamental en la gestión. Las actualizaciones corrigen vulnerabilidades y mejoran el rendimiento de los Access Points, routers y otros dispositivos de la red. Un programa de actualización periódica asegura que la red esté protegida contra las amenazas más recientes y que funcione con los últimos estándares de seguridad.

- **Pruebas de instalación y funcionamiento**

  Durante la instalación, se deben realizar pruebas parciales y continuas para asegurar que cada componente cumple con los estándares de calidad. Por ejemplo, al instalar cables de par trenzado o fibra óptica, se deben verificar parámetros de conexión y continuidad para asegurarse de que no haya errores en las conexiones. En la fase final, se realizan pruebas de rendimiento para confirmar que el sistema cumple con los requisitos de ancho de banda y calidad de señal.

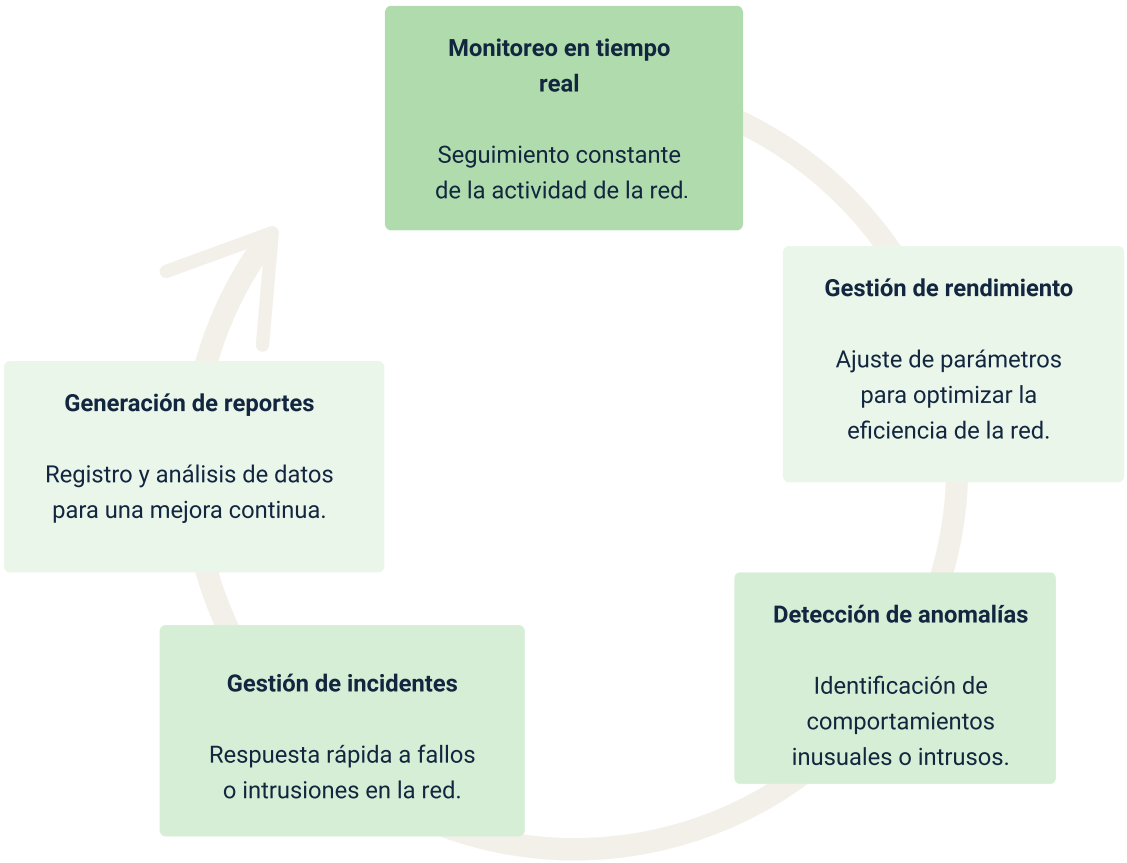
- **Documentación y reportes de calidad**

  El control de calidad incluye la documentación detallada de cada paso del proceso de instalación, así como los resultados de las pruebas realizadas. Esta documentación es valiosa tanto para los clientes como para el equipo de mantenimiento, ya que proporciona un registro de las condiciones iniciales del sistema y permite realizar futuras inspecciones o ampliaciones con mayor facilidad. Los reportes de calidad documentan los parámetros

de rendimiento alcanzados y validan que la instalación ha sido realizada conforme a los estándares.

Finalmente, el registro y almacenamiento de eventos de red son componentes esenciales de una estrategia de monitoreo y gestión efectiva. Los logs de red, o registros de eventos, permiten a los administradores realizar auditorías, investigar incidentes y analizar cualquier anomalía en el funcionamiento de la red. Mantener estos registros actualizados facilita la resolución de problemas, permite tener un historial de incidentes y mejora el control sobre el acceso a la red.

Figura 2. Ciclo de monitoreo y gestión en redes inalámbricas



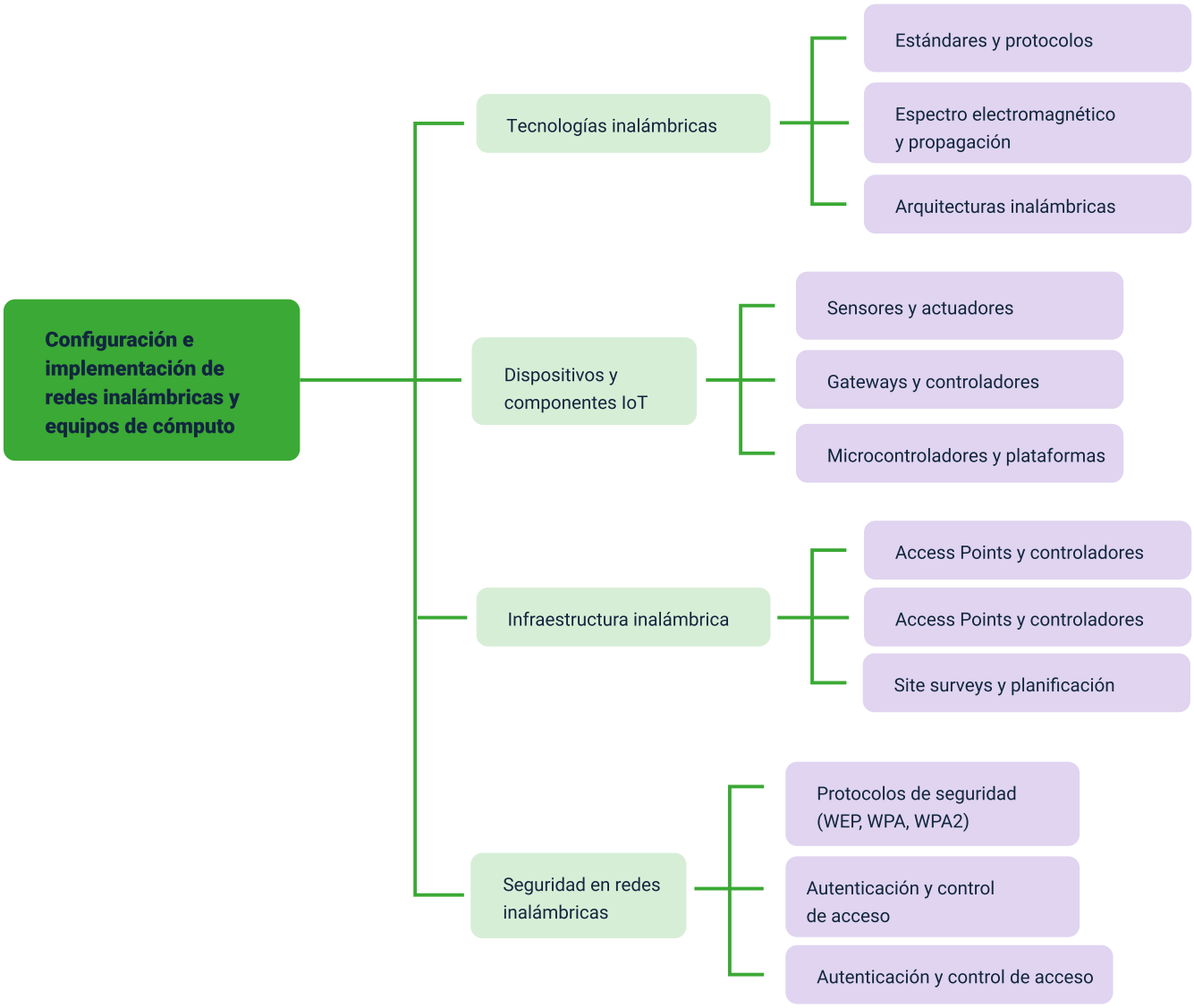
Fuente. OIT, 2024.

Síntesis

Este componente aborda los fundamentos y técnicas primordiales para la configuración, implementación y gestión de redes inalámbricas, así como los dispositivos de cómputo que las soportan. Comienza con un análisis de las tecnologías inalámbricas y sus estándares principales, como Wi-Fi, Bluetooth, y redes celulares 3G/4G/5G, que también explora conceptos de propagación en el espectro electromagnético y arquitecturas que sustentan estas redes.

Asimismo, se examinan los dispositivos que permiten el intercambio de datos de manera inteligente y eficiente en la red, considerando no solo los componentes básicos, sino también aquellos que habilitan funcionalidades avanzadas, como la integración de sensores y controladores. Esta interconectividad resulta fundamental en el contexto del Internet de las Cosas (IoT), donde los dispositivos deben operar en conjunto para lograr una red funcional, autónoma y escalable, capaz de sostener múltiples usuarios y aplicaciones.

Por último, se enfatiza en la importancia de la seguridad en redes inalámbricas, abordando tanto la protección de la infraestructura como la autenticación y control de acceso para los usuarios. Se presentan estrategias avanzadas de monitoreo y gestión que permiten supervisar y mantener la integridad de la red, asegurando que el acceso sea seguro y que el rendimiento se mantenga óptimo en todo momento.



Fuente. OIT, 2024.

Material complementario

Tema	Referencia	Tipo de material	Enlace del recurso
1. Tecnologías inalámbricas	Ecosistema de Recursos Educativos Digitales SENA. (2021, 25 junio). *¿Cómo funcionan las redes inalámbricas?* [Vídeo]. YouTube.	Video	https://www.youtube.com/watch?v=hyIpJZBLYg0
3. Infraestructura inalámbrica	Ecosistema de Recursos Educativos Digitales SENA. (2023b, octubre 30). *Site Survey* [Vídeo]. YouTube.	Video	https://www.youtube.com/watch?v=XaZJ3EYxQHU
2. Dispositivos y componentes IoT	Ecosistema de Recursos Educativos Digitales SENA. (2022, 11 marzo). *Arquitectura de internet de las cosas* (IoT) [Vídeo]. YouTube.	Video	https://www.youtube.com/watch?v=gaa-7nYolxE
4. Seguridad en redes inalámbricas	Ecosistema de Recursos Educativos Digitales SENA. (2023a, enero 30). *Herramientas de monitoreo y control* [Vídeo]. YouTube.	Video	https://www.youtube.com/watch?v=gp2cLOeucn4
4. Seguridad en redes inalámbricas	Contando Bits. (2024, 8 agosto). *Seguridad en Redes WIFI Protocolos WEP, WPA, WPA2 y WPA3* [Vídeo]. YouTube.	Video	https://www.youtube.com/watch?v=bloaGu5rl_I

Glosario

Access Point: dispositivo que permite la conexión inalámbrica de dispositivos a una red local, actuando como un puente entre dispositivos y el servidor o la red principal.

Actuador: componente de un sistema IoT que recibe señales y realiza una acción física en respuesta, como encender un motor, abrir una válvula o ajustar una luz.

Antena: dispositivo que transmite y recibe ondas de radio para la comunicación en redes inalámbricas, determinando en gran medida la cobertura y calidad de la señal.

Arquitectura inalámbrica: estructura y organización de los componentes y dispositivos de una red inalámbrica, incluyendo la disposición de access points, antenas y dispositivos terminales.

Autenticación: proceso mediante el cual se verifica la identidad de un usuario o dispositivo para permitir el acceso a una red o sistema de manera segura.

Bluetooth: estándar de comunicación inalámbrica de corto alcance diseñado para la transmisión de datos entre dispositivos de forma rápida y sencilla.

Cobertura: área geográfica en la que una red inalámbrica puede operar de manera efectiva y proporcionar conectividad a los dispositivos.

Controlador: componente de un sistema de redes o IoT que gestiona y coordina la operación de diversos dispositivos, asegurando que funcionen de manera sincronizada.

Espectro electromagnético: conjunto de todas las frecuencias de ondas electromagnéticas, desde ondas de radio hasta rayos gamma, utilizado en diversas tecnologías de comunicación, incluida la transmisión de datos inalámbricos.

Gateway: dispositivo que conecta redes diferentes entre sí, permitiendo la comunicación y transmisión de datos entre sistemas IoT y otros dispositivos o redes.

Gestión de incidentes: proceso de respuesta ante problemas detectados en la red, incluyendo acciones correctivas para restaurar el servicio y prevenir futuras interrupciones.

Microcontrolador: unidad de procesamiento de pequeña escala que integra una CPU, memoria y entradas/salidas en un solo chip, utilizado en dispositivos IoT para realizar tareas específicas de forma autónoma.

Monitoreo: actividad de supervisión continua de la red para identificar posibles problemas, caídas de servicio o intentos de acceso no autorizado, permitiendo respuestas rápidas.

Protocolo de seguridad: conjunto de reglas y algoritmos diseñados para proteger la comunicación en redes inalámbricas, como WEP, WPA y WPA2, asegurando que solo usuarios autorizados puedan acceder a la red.

Red inalámbrica: sistema de comunicación que permite la transmisión de datos sin necesidad de cables físicos, utilizando ondas electromagnéticas para la conexión entre dispositivos.

Sensor: dispositivo que detecta y mide condiciones físicas o químicas del entorno (como temperatura, presión o luz) y convierte esa información en señales que pueden ser interpretadas por otros dispositivos.

Site survey: proceso de evaluación de un sitio para planificar la implementación de una red inalámbrica, considerando factores como la cobertura, interferencias y ubicación de los access points.

WEP: protocolo de seguridad antiguo para redes inalámbricas, que en su momento ofrecía protección básica, pero ha sido reemplazado por opciones más seguras debido a sus vulnerabilidades.

WiFi: tecnología de red inalámbrica que permite la conexión de dispositivos a internet mediante la transmisión de datos a través de frecuencias de radio.

WPA/WPA2: protocolos de seguridad que mejoran la protección en redes inalámbricas respecto a WEP, proporcionando encriptación más avanzada para evitar accesos no autorizados.

Referencias bibliográficas

Alvear-Puertas, V., Rosero-Montalvo, P., & Peluffo-Ordóñez, D. (2017). Internet de las Cosas y Visión Artificial: Funcionamiento y aplicaciones: Revisión de literatura. Tomado de Internet de las Cosas y Visión Artificial, Funcionamiento y Aplicaciones: Revisión de Literatura

Bluetooth Special Interest Group (SIG). (2021). Bluetooth Core Specification Version 5.3. Bluetooth SIG. https://www.bluetooth.com/specifications/specs/core-specification-5-3/?form=MG0AV3

Durán, F. F., Mondragón, N., & Sánchez, M. (2008). Redes cableadas e inalámbricas para transmisión de datos. Científica, 12(3), 113-118. Tomado de Redalyc. Redes cableadas e inalámbricas para transmisión de datos

Flores Zermeño, F. J., & Cossio Franco, E. G. (2017). Aplicaciones, enfoques y tendencias del Internet de las Cosas (IoT): Revisión sistemática de la literatura. Tomado de Aplicaciones enfoques y tendencias del https://iot.pdf/?form=MG0AV3

González García, A. J. (2017). IoT: Dispositivos, tecnologías de transporte y aplicaciones: Trabajo final. Tomado de IoT: Dispositivos, tecnologías de transporte y aplicaciones

IEEE Standards Association. (2022). IEEE 802.11: Wireless Local Area Networks (Wi-Fi). IEEE Standards Association. https://standards.ieee.org/ieee/802.11/865/?form=MG0AV3

Jiménez Bonilla, Z. C., & Leaño Suárez, C. E. (2011). Redes inalámbricas: Diseño e implementación. Universidad Tecnológica de Bolívar. Tomado de Redes Inalámbricas: Diseño e Implementación

Karygiannis, T., & Owens, L. (2002). Wireless Network Security: 802.11, Bluetooth and Handheld Devices. NIST Special Publication 800-48. https://nistspecialpublication800-48.pdf/?form=MG0AV3

Rappaport, T. S., Heath, R. W., Daniels, R. C., & Murdock, J. N. (2014). Millimeter Wave Wireless Communications. Pearson Education.

Sharma, S. K., & Giannakis, G. B. (2020). Ultra-Reliable and Low-Latency Communications for 5G. IEEE Signal Processing Magazine, 37(2), 14-23. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8688469&form=MG0AV3

Wi-Fi Alliance. (2022). Wi-Fi Certified 6™ Release 2: Bringing Enhanced Features and Capabilities. Wi-Fi Alliance. Tomado de https://www.wi-fi.org/beacon/the-beacon/the-future-of-wi-fi-using-standardized-key-performance-indicators-and-evaluation

Créditos

Elaborado por:

Organización Internacional del Trabajo